PSR | Protective Security Requirements

New Zealand Government Security Classification System

Policy and guidance

New Zealand Government
Te Kāwanatanga o Aotearoa

Change log

Version	Published	Summary of key changes
1.0	1 Oct 2026	Consolidation of previous website content; no substantive policy changes.

Contents

Why classification matters

1. The New Zealand Government Security Classification System is owned and promoted by the Director-General of New Zealand Security Intelligence Service (NZSIS), which holds the Government's functional lead role as the Government Protective Security Lead (GPSL). Cabinet agreed to the Classification System in December 2000 [CAB(00)M42/4G(4)]. The Security and Intelligence Board (SIB) agreed to the 2022 policy on 23 March 2022.
2. The Security Classification System is the primary way that government information is protected. When used well, the Security Classification System can also enable and support appropriate sharing of government information and increase transparency and accountability to the public through systematic declassification and release.
3. The Security Classification System is mandatory for use by government departments, ministerial offices, the NZ Police, and the NZ Defence Force. The Security Classification System is mandated for use by mandatory requirement INFOSEC2 of the Protective Security Requirements (PSR) [CAB (14) 39/38]. To meet this mandatory requirement, your agency must implement the 2022 Security Classification system policy and requirements.

INFOSEC2 — Design your information security

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.

4. The Security Classification System is made available for use by all other government organisations as a best practice policy framework for classifying, handling and protecting government information. These organisations are encouraged to voluntarily adopt the Security Classification System.

What is government information?

5. Government information is all information, regardless of form or format, including documents, data, audio recordings and visual images. The New Zealand government collects, stores, processes, generates, or shares information 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.

6. Government information is a key strategic asset that enables both short-term and long-term outcomes that benefit all New Zealand and requires an appropriate degree of protection to keep it safe and available to those who need it. Government information therefore needs to be appropriately classified to achieve this result.

What is the Security Classification System?

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

8. Classification is the practice of assessing the sensitivity of the information and the likely harm that would result from the information being compromised.

9. All government information requires an appropriate degree of protection to ensure its continued integrity, availability, and confidentiality as required.

10. There are two types of government information.

    a. Information that would cause only minimal harm if compromised and does not need special Security or handling over and above the standard protections that apply to all government information. This is called 'Unclassified information'.
    b. Information that would cause harm to individuals, organisations, or New Zealand's national interest if compromised and needs specific Security measures to reduce the likelihood of compromise. This is called 'Classified information'.

11. The classification defines the sensitivity of the information (i.e. the likely harm that would result from its compromise) and defines the Security measures needed to protect it.

12. Note that a classification is a point-in-time risk assessment made by individuals. Classifications cannot themselves be used to justify withholding information; rather any request for information must be considered on its merits using harm criteria defined within the relevant legislation. See How to classify information for more information.

Why is classification important?

13. A classification and any other protective markings help to keep government information secure. Protective markings are a reminder of the sensitivity of the information or equipment and the security measures and special handling requirements that apply to it. It is important though to get classification right so that information is not:

    a. over-classified making its access or dissemination inappropriately restricted
    b. under-classified making it at-risk of being compromised and create harm for New Zealand or its allies.

14. Both situations are equally harmful to New Zealand and discussed in more detail in the How to classify information section.

Vision: A Security Classification System that protects and benefits all New Zealanders

15. To enable stewardship of government information for the benefit of all New Zealanders.

16. Our vision is to have a Security Classification System:

    a. that enables and supports the appropriate classification and systematic declassification of government information to improve government transparency and accountability to the public
    b. that enables information-sharing and purposeful collaboration between those who need it, when they need it
    c. where all government information is appropriately protected and used to its full potential
    d. where stewardship of government information benefits all New Zealanders.

The Security Classification System ecosystem

17. The Security Classification System plays a part within the New Zealand Government's information management and security ecosystem. The core components of that ecosystem are:

a. New Zealand legislation provides our legal obligations for collecting, accessing, handling, releasing, and managing government information appropriately. The main legislation supporting the Classification System includes the Official Information Act 1982, Public Records Act 2005, and Privacy Act 2020.
b. The Security Classification System provides a framework for assessing the impact of harm on people, organisations, or government if the information were compromised and defines the minimum requirements for secure handling of information to protect it.
c. Protective Security Requirements (PSR) (which includes the Security Classification System and New Zealand Information Security Manual (NZISM)) provides a framework for establishing appropriate protective security measures to protect people, information, and assets from harm and compromise. The classification level determines the minimum requirements for personnel, information, and physical security measures and controls defined within the NZISM and PSR.

Overview of the Security Classification System

18. The classification system includes the following components.

    a. Classifications set requirements for protective security measures to keep the information secure.
    b. Endorsements set requirements for special handling of the information and/or its dissemination.
    c. Secure handling requirements define the minimum protective security measures at each classification level.
    d. Classification system guidance and tools (this section of the PSR website) provide guidance to enable agencies to correctly use and apply the Classification System.
    e. Agency specific policies and procedures define the agency's specific classification policies and procedures describing how the generic classification system policies and requirements are applied in their specific context.

Protective marking

19. Protective markings are placed on government information and equipment to show the level of protection they need.

20. The protective marking shows:

a. that the information or equipment has been identified as sensitive in nature
b. the level of protection and special handling the information must have when it is produced, used, stored, shared, transmitted, carried, and disposed of
c. if the information has specific need-to-know access or usage requirement.

21. Protective markings can be applied to any public record, which includes (but is not limited to) documents, data, reports, letters, books, emails, meeting minutes, videos, audio recordings, verbal conversations, images, digital media, and information and communications technology (ICT) systems and equipment.

Protective markings include Classifications and Endorsements

22. Classifications determine the level of protections required to the information. Endorsements determine the special handling and need-to-know dissemination requirements.

23. When these markings are applied to government information or equipment, the information or equipment is referred to as being 'protectively marked'. See Applying protective markings to government information section for more information on how to protectively-mark information.

Classifications

24. Classifications set requirements for protective security measures to keep the information safe and secure. Classifications are divided into two categories.

a. Policy and privacy – classified to protect public interest or personal privacy.
b. National security – classified to protect the security, defence, or international relations of New Zealand.

Policy and privacy classifications

25. The classifications for government information that should be protected because of public interest, national policy, or personal privacy are below. See How to classify information section for more information.

IN-CONFIDENCE

26. Use the IN-CONFIDENCE classification when the compromise of information is likely to:

a. prejudice the maintenance of law and order
b. impede the effective conduct of government

c. adversely affect the privacy of New Zealand citizens.

27. For instance, when the compromise of information could prejudice:

    a. citizens' commercial information
    b. obligations of confidence
    c. measures for protecting the health and safety of the public
    d. the substantial economic interest of New Zealand
    e. measures that prevent or mitigate material loss to members of the public.

28. Or when a compromise of information could:

    a. breach constitutional conventions
    b. impede the effective conduct of public affairs
    c. breach legal professional privilege
    d. impede the government's commercial activities
    e. result in the disclosure or use of government information for improper gain or advantage.

SENSITIVE

29. Use the SENSITIVE security classification when the compromise of information is likely to damage New Zealand's interests or endanger the safety of its citizens.

30. For instance, where compromise could:

    a. endanger the safety of any person
    b. seriously damage the economy of New Zealand by prematurely disclosing decisions to change or continue government economic or financial policies relating to:
        i. exchange rates or the control of overseas exchange transactions
        ii. banking or credit regulations
        iii. taxation
        iv. the stability, control, and adjustment of prices of goods and services, rents, and other costs and rates of wages, salaries, and other incomes
        v. the borrowing of money by the New Zealand Government
        vi. the entering into of overseas trade agreements
        vii. impede government negotiations (including commercial and industrial negotiations).

National security classifications

31. The classifications for government information that should be protected because of national security are below. See How to classify information section for more information.

RESTRICTED

32. Use the RESTRICTED security classification when the compromise of information would be likely to adversely affect the national interest.

33. For instance, where compromise could:

    a. adversely affect diplomatic relations
    b. hinder the operational effectiveness or security of New Zealand or friendly forces
    c. hinder the security of New Zealand forces or friendly forces
    d. adversely affect the internal stability or economic wellbeing of New Zealand or friendly countries.

CONFIDENTIAL

34. Use the CONFIDENTIAL security classification when the compromise of information would cause significant damage to the national interest.

35. For instance, where compromise could:

    a. greatly damage diplomatic relations and cause formal protest or other sanctions
    b. damage the operational effectiveness of New Zealand forces or friendly forces
    c. damage the security of New Zealand forces or friendly forces
    d. damage the effectiveness of valuable security or intelligence operations
    e. damage the internal stability of New Zealand or friendly countries
    f. disrupt significant national infrastructure.

SECRET

36. Use the SECRET security classification when the compromise of information would cause serious damage to the national interest.

37. For instance, where compromise could:

    a. raise international tension
    b. seriously damage relations with friendly governments
    c. seriously damage the security of New Zealand forces or friendly forces
    d. seriously damage the operational effectiveness of New Zealand forces or friendly forces
    e. seriously damage the effectiveness of valuable security or intelligence operations
    f. seriously damage the internal stability of New Zealand or friendly countries
    g. shut down or substantially disrupt significant national infrastructure.

TOP SECRET

38. Use the TOP SECRET security classification when the compromise of information would cause exceptionally grave damage to the national interest.

39. For instance, where compromise could:

    a. threaten the internal stability of New Zealand or friendly countries
    b. lead directly to widespread loss of life
    c. cause exceptional damage to the security of New Zealand or allies
    d. cause exceptional damage to the operational effectiveness of New Zealand forces or friendly forces
    e. cause exceptional damage to the continuing effectiveness of extremely valuable security or intelligence operations
    f. cause exceptional damage to relations with other governments
    g. cause severe long-term damage to significant national infrastructure.

Endorsements

40. Endorsements warn people that information has special requirements. These are additional markings alongside the classification. These may include restricting access and dissemination based on need-to-know and special handling procedures. Agency specific policy and procedures will detail the endorsements used and any special requirements required for each endorsement.

41. 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.

42. You should use endorsement markings only when there is a clear need for special care. Remember that endorsement markings are not security classifications in their own right — they mustn't appear without a security classification.

Policy and Privacy endorsement markings

43. This section provides type of endorsement and their objectives applied to Policy and Privacy classifications.

APPOINTMENTS	This marking may be used before you announce actual or potential appointments, or during the deliberation stage of a recommendation and approval process.
BUDGET	This marking may be used for proposed or actual measures for the Budget before their announcement.
CABINET	This marking may be used for material that will be presented to, and/or require decisions by Cabinet or Cabinet committees.
COMMERCIAL	This marking may be used for commercially sensitive processes, negotiations, or affairs.
[DEPARTMENT] USE ONLY	This marking may be used for material intended only for use within the specified department(s).
EMBARGOED FOR RELEASE	This marking may be used on material before a designated time at which an announcement or address will be made, or information will be disseminated.
EVALUATIVE	This marking may be used for material about competitive evaluations, such as interview records and tender assessments.

HONOURS	This marking may be used for material about the actual or potential award of an honour. It may be used: • before the announcement of the award • during the deliberation stage of a recommendation or approval process • when you are considering honours policy matters involving the exercise of the royal prerogative.
LEGAL PRIVILEGE	This marking may be used for material that is subject to legal privilege.
MEDICAL	This marking may be used for material relating to: • medical reports • medical records and other material related to them.
STAFF	This marking may be used for material containing references to named or identifiable staff. It can also be used by staff for entrusting personal confidences to management.
POLICY	This marking may be used for material relating to proposals for new or changed government policy before publication.
TO BE REVIEWED ON	This marking may be used when the classification is to be reviewed at the designated time.

National Security endorsement markings

44. In addition to the Policy and Privacy endorsements in the section above, the table below provides additional endorsements and their objectives applied to National Security classifications.

ACCOUNTABLE MATERIAL	This marking shows that the information requires: • strict control over access and movement • regular auditing to ensure its safe custody (use a risk assessment to decide how often to audit). What constitutes ACCOUNTABLE MATERIAL will vary from agency to agency. Note TOP SECRET information is ACCOUNTABLE MATERIAL by default.
NEW ZEALAND EYES ONLY (NZEO)	This marking indicates that access to information is restricted to New Zealand citizens with an appropriate security clearance on a need-to-know basis.

	For government information carrying the endorsement marking NZEO and the security classification of IN-CONFIDENCE, SENSITIVE, or RESTRICTED: • If an agency head considers that foreign nationals should be given information marked NZEO, the agency head must consult with the originating agency to see if the endorsement marking is still required or whether it could be modified to enable release. It may be possible to have the endorsement marking removed or to release part of the information by removing the endorsement marking. For government information carrying the endorsement marking NZEO and the security classification of CONFIDENTIAL, SECRET or TOP SECRET: • Foreign nationals must not be allowed access, even if they have the appropriate New Zealand security clearance. However, in limited circumstances, agencies may allow information marked NZEO to be viewed by appropriately cleared foreign nationals where there is an essential business need. In all such circumstances, the Director-General of the New Zealand Security Intelligence Service must grant approval for this access. Use this marking with caution. This marking requires the agency to track and restrict information access and dissemination based on the nationality and/or waivers in place before allowing dissemination or access. This endorsement should be used with caution as the effort for implementing the security controls can be high. It also requires organisations to restrict who can manage and support the information and systems with NZEO markings. When the information is disseminated to different agencies, it extends the same requirements to all agencies who have access to or receive the information.
RELEASEABLE TO (REL TO)	This marking identifies information that is releasable to the countries or citizens of those indicated countries only. For example, RELEASABLE TO//NZL, GBR or REL TO//NZL, GBR means that the information may be passed to citizens and the governments of the United Kingdom and New Zealand only. You must use the appropriate three-letter country codes from the SAI-Global – ISO 3166-1 Codes to represent country names and their subdivisions. See 'Part 1: Country codes'.

	For example, common nation tri-graphs are: NZL, AUS, CAN, GBR, USA. Convention is for originating agency to be listed first, so NZL would be listed first, and the remainder in alphabetical order.

Sensitive compartmented markings

45. A sensitive compartmented marking is a word indicating that the information is in a specific need-to-know compartment. This word could be a codeword or 'Sensitive Compartmented Information (SCI)'.

46. A compartmented marking is a special type of National Security endorsement marking.

47. It is often necessary to take security precautions beyond those normally indicated by the security classification to protect compartmented information.

48. The agency that owns the information specifies what the extra precautions are.

49. See also Applying national security endorsement markings.

How to classify information

50. Classifying government information must be based on a ‘harm test’. If your assessment shows that compromise of information would have adverse results, you must:

    a. classify and protectively mark the information
    b. give that information extra protection in line with the severity of the likely damage.

Classification and Business Impact Levels

51. The Classification System uses Business Impact Levels (BILs) as a standard tool to assess the impact that might occur if its confidentiality, integrity or availability is compromised.

52. The BIL scale ranges from 1 (low) to 6 (catastrophic) impacts. The higher the impact, the stronger your security measures must be.

53. Although agencies should apply their own judgement in every case, the likely relationship between the harm test and classification level is shown in the table below.

Business Impact Levels (BIL) Matrix (Assessing the impacts of a compromise of the information)

Table 2: Business Impact Levels

		Policy & Privacy Information that should be protected because of national interest, national policy, or personal privacy.		**National Security** Information that should be protected because of the national interest, security, defence, or international relations of the Government of New Zealand			
Business Impact Level	**1-LOW**	**2-MEDIUM**	**3-HIGH**	**3-HIGH**	**4-VERY HIGH**	**5-EXTREME**	**6-CATASTROPHIC**
Classification	**UNCLASSIFED**	**IN-CONFIDENCE**	**SENSITIVE**	**RESTRICTED**	**CONFIDENTIAL**	**SECRET**	**TOP SECRET**
Personal Impact An individual's rights, freedoms, health, or safety	Causing low impact to a person.	Breaching a person's privacy causing non-serious or life-threatening harm. Impeding with activities that protect health and safety and any other personal legal protections.	Endangering the safety of a person. Affecting an individual's wellbeing and/or livelihood.	N/A	N/A	N/A	N/A
Organisational Impact Organisation operations, finances, reputation, or obligations under NZ law	Causing low impact to an organisation.	Breaching organisational obligations to keep some information protected, e.g.: • 'Free and frank' advice • Legal and other professional privilege • Obligations of confidentiality, e.g. commercial agreements • Constitutional conventions of confidentiality and political neutrality.	Causing disruption to operations (or organisational assets) to the extent that an organisation can't perform one or more primary functions. Causing a loss of trust in the organisation with members of the public and/or other stakeholders. Breaching organisational obligations that result in formal investigation and/or prosecution.	N/A	N/A	N/A	N/A
New Zealand Domestic Impact National services or infrastructure, New Zealand's economy, and maintenance of law and order	Causing low impact on national services and infrastructure. Causing low impact on the maintenance of law and order or the New Zealand economy.	Impeding non-critical operations of national infrastructure and/or services. Impeding the preservation of law and order.	Prematurely disclosing information on government policies that has economic or financial consequences. Affecting national services or the security or resilience of national infrastructure.	Adversely affecting economic, scientific, or technological matters vital to New Zealand's stability and integrity. Degrading the ability to prevent, detect and investigate offences.	Causing harm to confidence in the New Zealand Government. Causing harm to the ability to prevent, detect, or investigate offences. Causing significant harm to the financial viability or productivity of a significant sector of the economy. Causing significant harm to, and short-term shut down of, critical national infrastructure (days to weeks).	Causing serious impact to the maintenance of law, regarding the prevention, investigation, and detection of serious or international organised crime. Causing serious disruption on the ability of Government to provide effective services to the public. Causing serious damage to all parts of the economy. Causing serious disruption and medium-term shut down of critical national infrastructure (weeks to months).	Causing significant failure to operate within the rule of law, resulting in long-term damage to public order, democracy, and human rights. Causing catastrophic failure in the ability to maintain the law. Causing widespread and lasting breakdown in the ability of Government to provide public services. Causing exceptionally grave or long-term impact on the New Zealand economy. Causing permanent damage or long-term shutdown of critical national infrastructure (months to years).
National Security Impact Defence, Security, and International Relations	Causing low impact on defence, national security, and international relations.	N/A	N/A	Degrading the effectiveness of agencies working in national security. Degrading the operational effectiveness or security of New Zealand or allied forces, such that operations may need to be replanned, reprioritised, or delayed. Adversely affecting New Zealand's diplomatic relations, e.g., affecting negotiations with a nation.	Causing harm to the operational effectiveness or security of New Zealand or allied forces, e.g. • short term reduction in operational effectiveness or security of New Zealand or friendly forces • cause short term or significant impact to non-critical national security services and intelligence operations. Causing harm to the international reputation and diplomatic relations of New Zealand e.g., resulting in formal protest from other nations or compromising NZ's interests in a bi-lateral trade negotiation.	Causing serious harm to the operational effectiveness or security of New Zealand or allied forces, e.g. • current or future military capability or installations would be rendered unusable • serious damage to critical security services and intelligence operations would happen. Causing serious damage to diplomatic relations with friendly Governments. Severely disadvantaging New Zealand in international negotiations.	Causing exceptionally grave or long-term damage to the security or operations of New Zealand or allied forces, e.g. to the operational effectiveness of New Zealand or allied forces. Causing long-term damage to the effectiveness of intelligence, security, or counter-terrorism operations. Threatening the stability of New Zealand and/or friendly countries. Causing exceptional damage to relations with other Governments.

Assess the harm

54. To assess the harm, use the BILs matrix and the following guide to identify and articulate the harm.

55. When assessing the harm of compromise ask yourself the following two questions.

    a. Who or what would be impacted by compromise of the information?
    b. How much of an impact would compromise of this information cause?

Who or what would be impacted by compromise of the information?

56. The Business Impact Levels matrix considers impacts in four categories: Personal; Organisational; New Zealand domestic; and, Defence, Security and International Relations.

57. Identify which categories apply for the information in question.

58. Note: When classifying information, the information set may touch on multiple categories. The harm test should cover all relevant categories for the information set(s) in question.

Category	Identifying Questions
Personal Impact	If the information was compromised, would it have any impact on a person's rights, freedoms, health or safety under New Zealand law e.g.: • breach their privacy • affect their wellbeing or livelihood • endanger their safety?
Organisational Impact	If this information was compromised would it affect or harm an organisation's operations, finances, reputation, or obligations under New Zealand law?
National interests: New Zealand Domestic Impact	If this information was compromised would it have any impact on New Zealand national services, national infrastructure, economy, or the maintenance of law and order?
National interests: Defence, Security and International Relations Impact	If this information was compromised would it have any impact on New Zealand's defence, security, or international relations or on friendly nations?

59. User tip: When assessing harm, it can be useful to search if the information is already publicly available. If already available publicly, then compromise of the information is likely to have low impact.

How much of an impact would compromise of this information cause?

60. For each of the impact categories you identified in Q1, assess the harm level against the BILs Matrix.

61. User tip: When authoring or preparing information with information at different classification levels, consider use of paragraph marking to clearly identify the classification of each section of a document, email, or dataset. This articulates the sections that have the highest classification level and enable more appropriate information sharing with different audiences

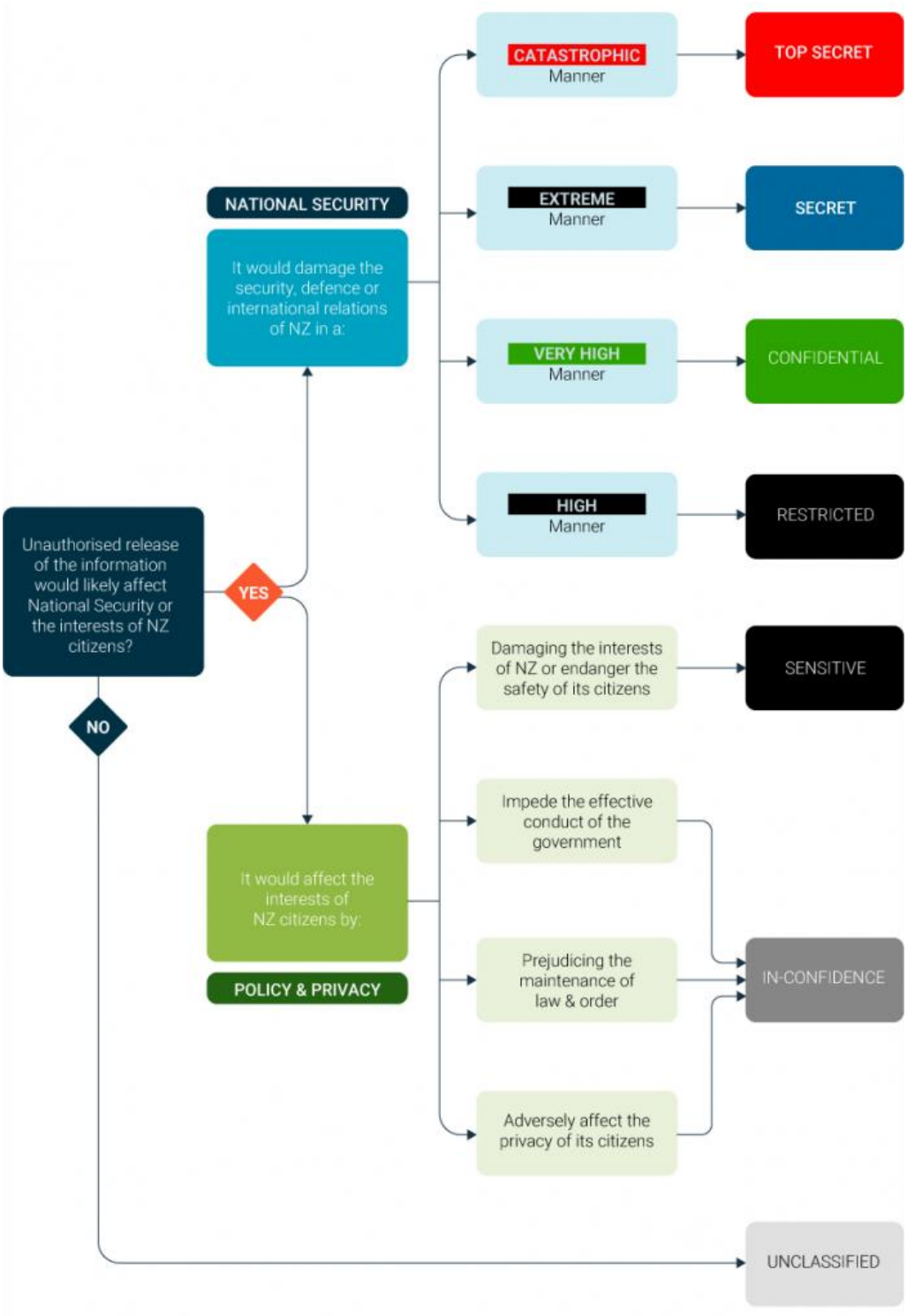
62. When information is aggregated together into a collection (e.g. within a document, database, or system), you must use (at minimum) the highest classification level of any paragraph marking for the entire information collection. Note that aggregation of classified information may require increased protection as the harm and impact of its compromise may be higher.

63. The BILs use a continuum of increasing impact from (1) Low to (6) Catastrophic. The judgement that users must make when assessing harm can be subjective. The Classification Tool below is provided to help distinguish these levels and assess the appropriate business impact level.

64. If the information would not cause harm to New Zealand's national interests, then begin your assessment at Policy and Privacy 3 High Impact.

Classification flow chart

65. For experienced classifiers, use the Classification flow chart to quickly help you assess harm and impact and classify information.



66. The rest of this section provides more guidance, scenarios, and considerations to enable you to make an informed and appropriate classification decision.

67. User tip: An agency's context, information sets, and harm scenarios can be nuanced and unique. Agencies should ensure that their classification policies and procedures contextualise their specific information sets and classification choices to make it easier for their people to make appropriate classification decisions for their specific information sets and scenarios.

Scenario 1:
Names and contact details for workshop attendees

68. A government agency runs a series of regional workshops on construction safety and collect the names and contact details of everyone who attends.

69. Attendees are predominantly health and safety managers in construction firms or other health and safety professionals. As part of the registration process, attendees consented to have their names and locations shared across the health and safety community. Carlo works for the government agency and wants to classify this information. He believes that there is no risk of real harm if the list was released so he is happy it is not SENSITIVE. However, he knows that the release of people's personal information can cause trouble and is considering classifying the document as IN-CONFIDENCE.

70. Is he right?

71. This information can be marked as UNCLASSIFIED. All individuals have privacy rights that are defined in the Privacy Act 2020 and must be protected accordingly. Not all personal information requires classification to increase protections beyond the standard protections applied to all personal information. Compromise of this information is unlikely to result in a privacy breach.

Scenario 2:
Record of an investigation into an individual for wrong-doing

72. A whistleblower alleged to the agency's finance manager that an individual currently working for the agency was committing financial fraud. An investigation file was opened to ascertain the validity of the claim.

73. The staff member creating the investigation file is clear that release of this information would, at the least, cause distress and that it should be at least IN-CONFIDENCE. However, given the nature of the information the staff member agreed with the manager that it should be classified as SENSITIVE.

74. Are they right?

75. Yes. It is reasonable to assume that the release of this information could harm someone's well-being. On the basis of the harm test, this information should be SENSITIVE.

Classification considerations

76. This section provides general tips and things to consider when classifying.

Who should classify information?

77. The person or agency responsible for creating or preparing the information decides its classification and protective marking. This person or agency is called the 'originator'.

78. If information is created outside the New Zealand Government, the person working for the government organisation who actioned the information should determine whether it requires a protective marking.

79. To classify, the first step is to assess the harm and impact if the information is compromised.

Justify before you classify

80. Classification is not 'free'. As the classification level increases, information becomes harder to manage and harder to use. It is important that information is classified correctly and that higher levels of classification are only used for information whose compromise would cause higher levels of harm.

81. The concept of 'justify before you classify' asks everyone who makes classification decisions to confirm their reasoning before classifying information. This isn't a formal process, just an expectation that classifiers of information make a conscious choice every time they classify.

Over-classifying information is harmful

82. Over-classifying information can be harmful such as:

    a. public access to government information can become unnecessarily limited
    b. unnecessary administrative arrangements are set up that remain in force for the life of the information which imposes an unnecessary cost on the agency
    c. classified records, CONFIDENTIAL or higher, cannot be transferred to Archives New Zealand. They will need to be retained by the agency and if not eventually declassified will require a deferral of transfer from the Chief Archivist possibly indefinitely

d. the volume of protectively-marked information increases requiring larger secure storage facilities and secure systems to maintain the security controls
e. the Classification System and associated security procedures are brought into disrepute
f. persistent over-classification can lead to protective markings being devalued or ignored.

Unclassified information must still be protected

83. All of government information requires an appropriate degree of protection to keep it secure, available, and accurate. This includes unclassified and publicly available information. Agencies must apply appropriate standard protections for all government information they assess necessary based on their security risks and threats.

84. UNCLASSIFIED isn't a security classification, but it is used as a protective marking to show that the impact from unauthorised disclosure or misuse has been assessed as low and standard protections are sufficient to keep it secure.

85. Your organisation should have policy on how you will mark, protect, and handle information that needs increased protection but doesn't qualify for a security classification.

86. User tip: if there is no protective marking on government information you receive or access, do not assume it is unclassified. Read the information and do your own harm assessment as the originator may have made a mistake.

SENSITIVE information includes threat to life

87. Policy and privacy categories should not be considered as 'less serious' than the national security classifications. The compromise of SENSITIVE information could still result in loss of life for an individual, e.g. if the contact details of police informers were released.

88. Some information is not about national security but could still result in the loss of life and other serious harm.

Information from other sources

89. Protective markings suggested by outside organisations or individuals should not automatically be accepted by New Zealand government agencies unless there has been a prior agreement.

90. Information derived directly from protectively-marked sources must carry, at a minimum, the highest security classification of any of the source classifications.

91. However, if you suspect that the protectively-marked sources are no longer correctly classified, it may be time for the source information to be reviewed. Contact the owning organisation to clarify and agree the correct classification and protective marking for the information.

Identifying national security information

92. National security information is defined as any government information or resource (including equipment) that records information about, or is associated with, New Zealand's:

    a. protection from espionage, sabotage, violent extremism, promotion of communal violence, attacks on New Zealand's defence system, acts of foreign interference, acts of malicious cyber activity
    b. protection of territorial and border integrity and security from serious threats (including maritime, air, ocean, fishing, other natural resources, cargo, mail systems, and international aviation)
    c. defence plans and operations
    d. intelligence community capability and operations
    e. regional security and stability matters in Asia and Pacific regions (including geostrategic competition, corruption, people trafficking, and transnational organised crime)
    f. international relations and foreign policy positions in our interest (significant political and economic relations with international organisations and foreign governments)
    g. law enforcement operations (where compromise could hamper or make useless national crime prevention strategies or particular investigations; or adversely affect personal safety)
    h. national interest (relating to economic, scientific, or technological matters vital to New Zealand's stability and integrity).

93. See also: New Zealand's National Security Intelligence Priorities (dpmc.govt.nz).

Does all national security information need to be classified?

94. National security information should only be classified and protective-marked if its compromise could damage national security, the New Zealand government, commercial entities or members of the public.

National security scenario

95. A New Zealand industry is highly significant to the national economy and its success depends on some copyrighted technologies which international competitors do not have access to. In this scenario, the compromise of trade secrets could have a material impact on New Zealand's stability, and this would be

national security information (and require a minimum classification of RESTRICTED).

How to protectively mark classified information

96. 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.

97. These requirements for securely handling government information applies to all government information, with or without a security classification.

98. Protective markings are not just for paper documents – they're also for electronic information, digital media, information that will be delivered verbally, and equipment in which protectively-marked information is held or stored.

99. See also Classification Quick Guide.

Applying protective markings to government information

100. Protective markings are placed on information and equipment to show the level of protection they need. Once you've identified information or equipment that needs protection or special handling (or both), you must assign a protective marking to it.

101. 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.

102. How to apply protective markings depends on the how and where the information is created, stored, accessed, and used. For example, protective markings go at the top and bottom of each page of a document. A document means any form of recorded information, such as reports, letters, books, email, minutes, memoranda, films, charts, tapes, images, and digital media.

103. When printed documents are filed, their protective markings should be clearly visible. The same rule applies to removable electronic and optical media, such as USBs, CD-ROMs, microfilms, photographs, and removable hard drives.

104. Protective markings include Classifications and Endorsements.

Who sets and controls protective marking?

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

106. When information is created, the originator must do a risk assessment of the harm or prejudice that would result from specific content or equipment being compromised. If adverse consequences could occur, or the agency is legally required to protect the information, it must be given a protective marking.

107. Protective markings suggested by outside organisations or individuals should not automatically be accepted by New Zealand government agencies unless there has been a prior agreement.

108. Information derived directly from protectively-marked sources must carry, at a minimum, the highest security classification of any of the source classifications.

Who can change protective markings?

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

110. Only the agency that assigns the original protective marking (the originating agency) can change it. All agencies must respect this rule.

111. Originating agencies should ensure that information shared with other agencies and partners are informed of changes to protective markings and does not withhold information inappropriately.

112. However, if you assess that the information is over-classified, you should seek agreement to remove or change a protective marking. If the originating agency doesn't agree to remove the marking, the information should not be released. If the requirement to release the information is subject to an official information request, an agency may transfer a request to another agency to fulfil the request should the information be held by the originating agency. See the Office of the Ombudsman (ombudsman.parliament.nz) for more information on official information request transfers.

113. However, the absence of permission to release or acceptance of transfer from the originating agency does not absolve the receiving agency of the obligation to decide on the request. The agency should use the tools provided in the Ombudsman's guidance to assess the harm of disclosure against the public interest. This does not prevent the agency from consulting other interested parties before making the decision.

What to do if the owning organisation is disestablished or merged

114. If an agency is disestablished or merged, the agency assuming the former agency's responsibilities is considered the owner.

115. The point of contact should be the Chief Security Officer (CSO) of the new agency.

What happens when information goes to Archives New Zealand?

116. Archives New Zealand has limited capacity to store protectively-marked information, so consult with them first. If they can't accommodate your information, seek leave to defer the transfer of protectively-marked records in line with the Public Records Act 2005.

117. If your agency is considering transferring records marked CONFIDENTIAL or above, consult with Archives New Zealand about declassifying the protective marking to a more relevant level.

118. Access to public archives in the control of the Chief Archivist is governed by an Access Authority set by the controlling public office and not the markings themselves. This access authority should take the protective markings into account, but it is the Access Authority which determines access. Handling and storage is consistent across all holdings regardless of the markings and meets the requirements of records marked at RESTRICTED.

119. When a record has been marked under the Public Records Act 2005 as being an open access record, any protective markings cease to have effect for any purpose.

120. See also How to declassify information.

Releasing government information to the public

121. New Zealand government employees must have agency authorisation to release any information to members of the public, regardless of any protective marking it may or may not have.

122. Authorisation may be granted by the agency head or a person given delegated authority by the agency head.

123. Even if information is intended for public release or publication, it may carry a control measure, such as an endorsement marking before its release. For example, Budget papers.

124. In this case, the point at which the information will be publicly available should be marked. When this information ceases to require the original control measures, your agency should consider applying protection measures consistent with the type of information contained within the document.

125. All personal information held, even if it is publicly available, must be handled in line with the Privacy Act 2020, Information Privacy Principles.

126. For records transferred to Archives New Zealand the agency remains responsible for managing requests to access or release of information restricted under their access authority.

Handling requests for official information

127. Your agency should have policy in place for addressing every request for government information, which may be released under the Official Information Act 1982 (OIA).

128. Understanding the legislation and implementing agency-specific OIA policy reduces the likelihood of an official information security breach through unintended or accidental disclosure.

How to protectively mark information and equipment

Applying Classifications

129. Security classifications must be marked in bold and in capitals. They should be at the same size as the body text or at least 3mm high (whichever is larger).

Colour-coding security classifications

130. Colour coding makes security classifications easier to identify and ensures higher classifications stand out.

131. Colour-code security classifications as follows:

UNCLASSIFIED	Marking is recommended
IN-CONFIDENCE	**BLACK**
SENSITIVE	**BLACK**
RESTRICTED	**BLACK**
CONFIDENTIAL	**GREEN** (RGB 0,176,80)
SECRET	**BLUE** (RGB 0,0,255)
TOP SECRET	**RED** (RGB 255,0,0)

Applying Policy and Privacy endorsement markings

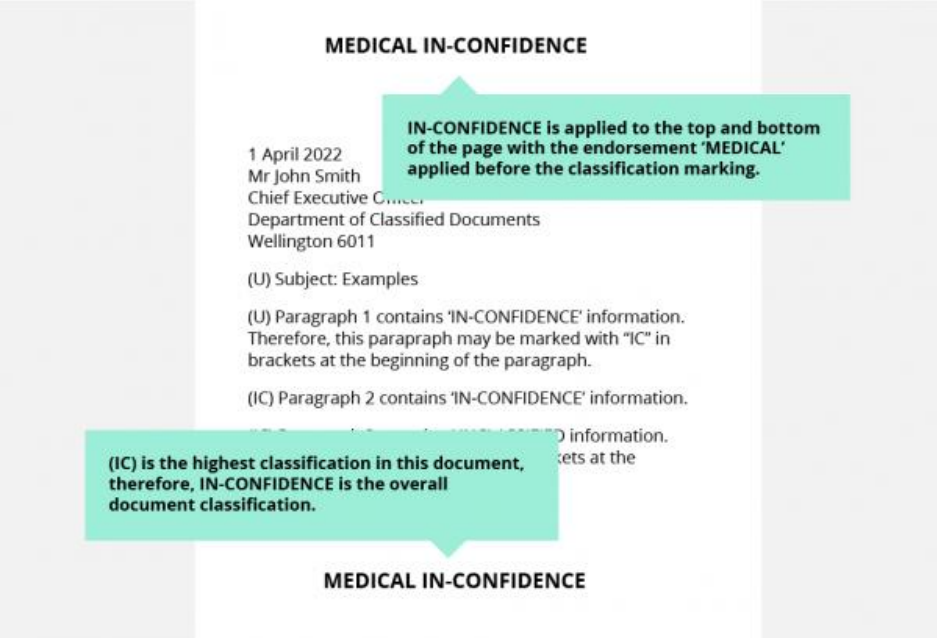
132. You must not use endorsement markings without a security classification.

133. Endorsements are applied differently between Policy and Privacy Classifications (IN CONFIDENCE or SENSITIVE) and National Security Classifications (RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET).

134. When applying an endorsement marking to Policy and Privacy Classifications, it is combined with the security classification as follows:

    a. Same style, font and size as the classification marking
    b. Appears before the classification marking.

135. For example:



Applying National Security endorsement markings

136. National Security endorsement markings must follow a security classification. Don't apply them to information that doesn't have a security classification.

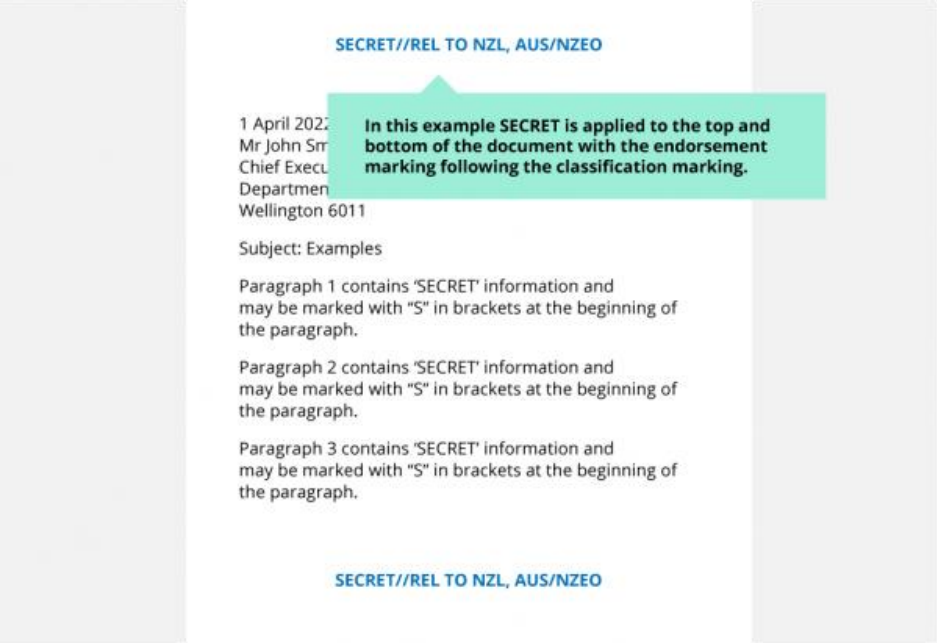
137. National security endorsement markings are generally categorised into control markings and dissemination markings. SCI is a type of control marking. See your agency specific classification policy and procedures for the specific control and dissemination markings used in your organisation or sector.

    a. The endorsement marking (including any SCI markings) is combined with the classification marking as follows:
    b. Same style, font, size and colour as the classification marking
    c. Appears after the classification marking
    d. Use a double forward slash between the classification, control, and dissemination marking categories

e. If there are multiple markings to apply within each category, separate them with a single forward slash.

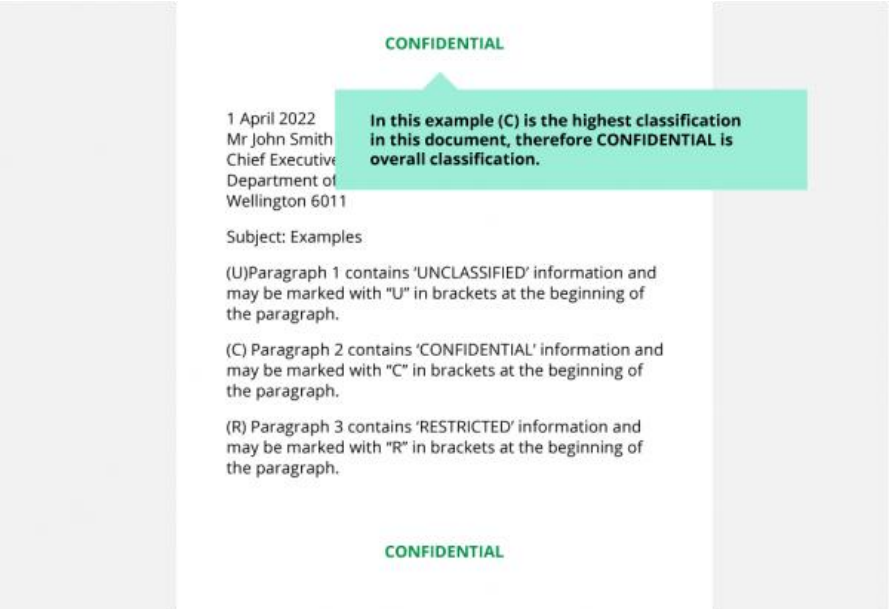
138. The format is:
CLASSIFICATION//CONTROL 1/CONTROL 2//DISSEMINATION 1/DISSEMINATION 2

139. For example:
TOP SECRET//<SCI CODEWORD>//ORCON/REL TO NZL, FVEY



Marking documents

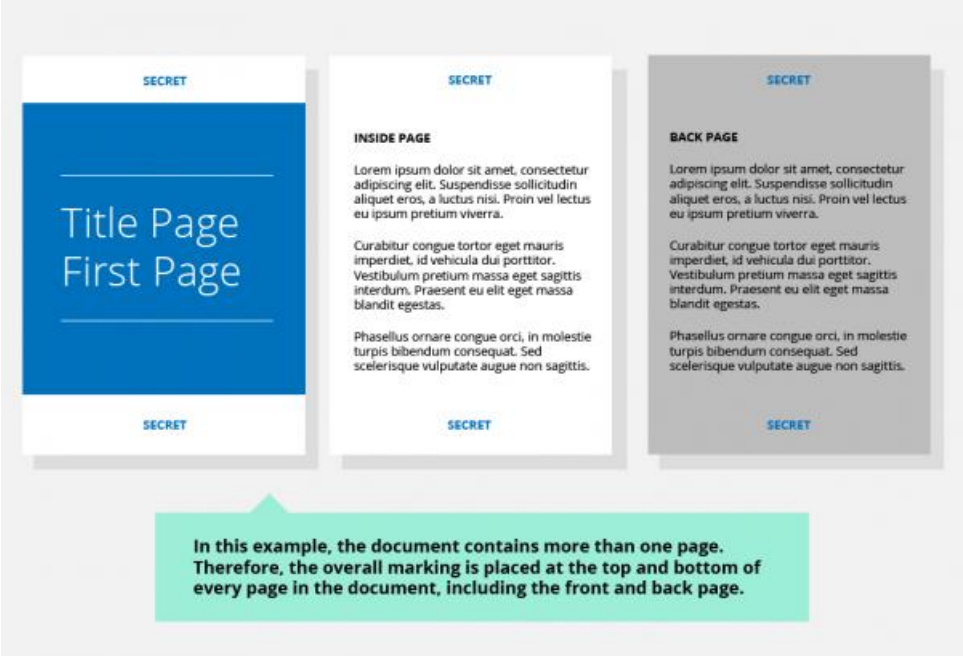
140. When protectively marking documents, the highest security classification should be clearly marked in bold at the centre top and bottom of each page in a single line as shown in Example 3.



141. If necessary, the security classification can be stacked in the centre of the page to fit around a letterhead.

142. Documents with covers, or in folders, must show the security classification on:

    a. the front and rear covers
    b. the title page
    c. all other pages in the document.
    d. Any bindings or fastenings must not obscure the protective marking.



Marking paragraphs

143. Sometimes paragraphs may need to be marked because they have different or higher security needs. For example, a paragraph in a document might contain secret information. Paragraph markings are called ‘paragraph grading indicators’.

144. Your agency should consider including in your classification policy and procedures, information on protectively-marking paragraphs.

Applying paragraph grading indicators

145. Put paragraph grading indicators in brackets at the beginning of each paragraph. Write them in full or abbreviate them using the first letters of the security classification. For example, (S) for SECRET or (IC) for IN-CONFIDENCE. Table 8 shows the standard abbreviations you can use.

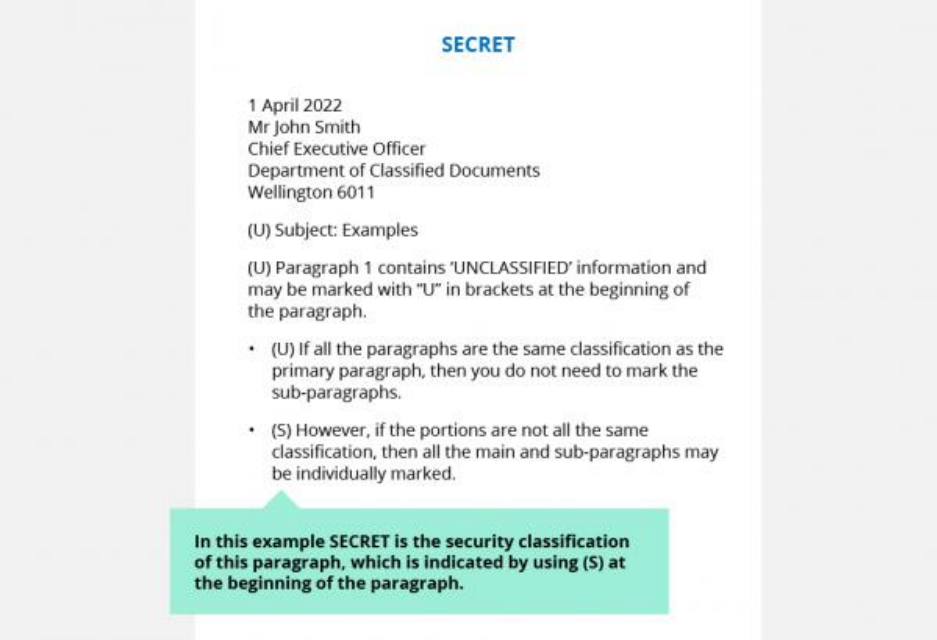
146. Paragraph grading indicators should be the same colour as the text in the document.

147. If you use paragraph grading indicators, you must also mark all the paragraphs in the document, so that no one is confused about which markings apply to what text.

148. Use UNCLASSIFIED for paragraphs that don't carry a protective marking.

Abbreviated security classifications

UNCLASSIFIED	(U)
IN-CONFIDENCE	(IC)
SENSITIVE	(Sen)
RESTRICTED	(R)
CONFIDENTIAL	(C)
SECRET	(S)
TOP SECRET	(TS)



149. Once you've applied paragraph grading indicators, you need to establish the overall protective marking for the document. The overall marking must be at least equal to the highest classification level of any one paragraph within the document.

Marking books, pamphlets, and reports

150. Documents with covers, such as books, pamphlets and reports, must show the protective marking on:

    a. each page
    b. the front and rear covers
    c. the title page
    d. the binding (if possible).

151. Any binding or fastening of pages must not obscure the protective markings.

Marking titles

152. Whenever possible, don't put protective markings on titles of things like files, documents, books, and reports. They could be seen in management systems that aren't protectively marked, and this could put the information at risk.

153. If marking the title is essential, the originator should use a separate UNCLASSIFIED reference. This mark can appear behind the title in brackets.

Marking printed graphics

154. For graphics such as maps and drawings:

    a. print or stamp the protective markings near the map scale or drawing numbers
    b. print the protective markings at the top and bottom centre of the graphic.
    c. if the graphic will be folded, make sure the marking remains visible after folding.

Marking annexes, appendices, attachments, and covering documents

155. In some cases, the annexes or appendices to a document need protective markings even if the rest of the document is UNCLASSIFIED.

156. Occasionally, an annex or appendix may also need a different protective marking from the principal document it is attached to.

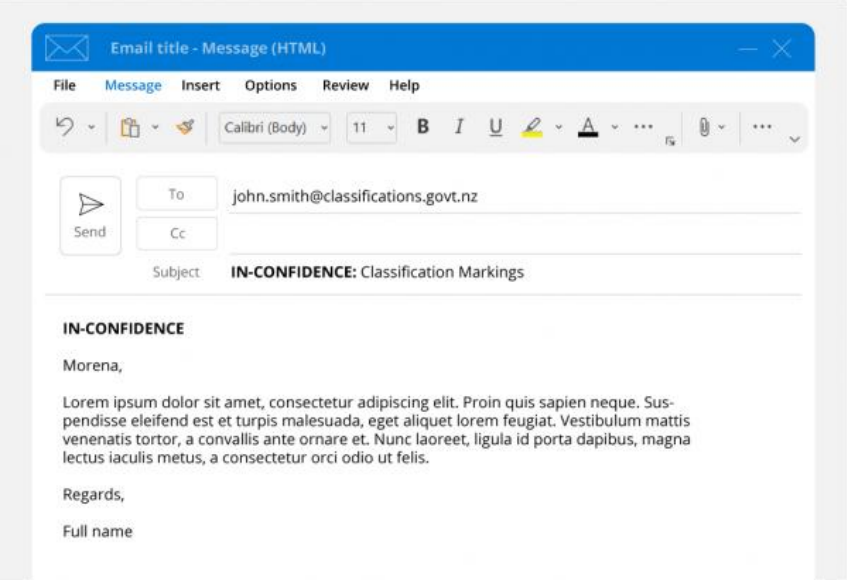
157. If the annex, appendix, or attachment has a higher protective marking than the principal document, the document's front cover should indicate that the document as a whole has a higher security classification. Example 6 shows you how to mark correctly in this scenario.

158. If the annex, appendix, or attachment is at the same protective marking level as the principal document or lower, you don't need to show that on the cover.

Marking emails

159. Emails should be marked with an appropriate protective marking. The markings need to clearly show how the information is to be treated, so that the level of security around the email is obvious to the viewer. This may be capitalised as the

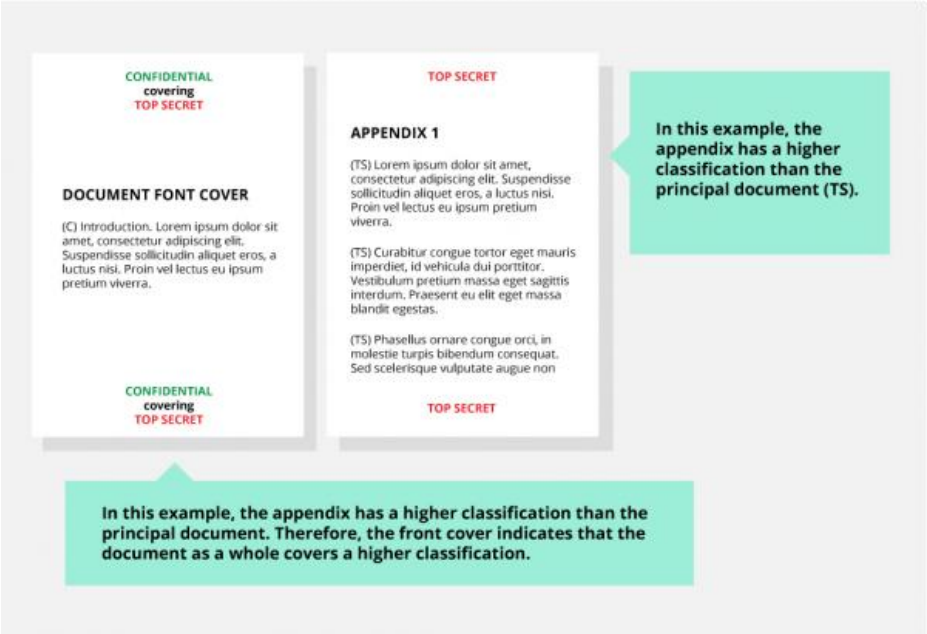
first word in the subject line and at the top of the page in the content of the email, often with a larger font size and bolded text to display the classification.



160. TOP SECRET, SECRET, or CONFIDENTIAL information cannot be sent via email unless it is on a GCSB accredited system.

161. Marking emails ensures that:

    a. the intended audience understands their obligations for securely handling the information
    b. appropriate security measures are applied to the information
    c. information isn't being accidentally released into the public domain.



162. Clearly marked content should easily convey the security level of the email, which can be shown through a classification easily identifiable in the subject line or at the top of the text. For more information on best practice for email security please see:

    a. Government Digital Delivery Agency (digital.govt.nz)
    b. NZISM Email Security (nzism.gcsb.govt.nz).

Marking imagery

163. Photographs and film, and their storage envelopes or containers must all carry clear protective markings when applicable.

164. Protective markings must be:

    a. on both sides of containers and spools
    b. projected for at least five seconds in the title and end sequences of roll imagery, cine-film, and video tape.

165. You must also mark photographic negatives, so that the protective marking is reproduced on all copies made from that negative.

Marking presentations

166. Official presentations and presentations with security classifications presentations need appropriate protective markings.

167. Treat each slide or screen as an individual page, as you would for a paper-based document. The protective marking should be verbally stated to the audience.

Marking audio

168. For audio recordings, the level of protective marking must be clearly stated at the beginning and end of each recording. The tape or other media and its container must be conspicuously labelled with the appropriate protective marking.

Marking microforms

169. Some agencies may still hold microforms such as aperture cards, microfiche, and microfilm that contains protectively-marked information. If so, this material must show the appropriate protective marking at the top and bottom centre of each frame.

170. Containers and envelopes must bear the appropriate protective marking of the highest protectively-marked microform.

171. The protective marking must be visible without projection on cards and microfiche. Microfilm should be prominently marked at the beginning and end of each roll.

Marking electronic storage media

172. For the policy on marking electronic storage media, please see 12.3 Product Classifying and Labelling (nzism.gcsb.govt.nz) and 13.2 Media Handling (nzism.gcsb.govt.nz).

Marking equipment or storage media

173. Your agency must develop specific procedures for marking equipment and electronic storage media. Protective markings should be clearly visible and not easily removed.

How to protect classified information

174. Protecting information with protective markings must be controlled and handled correctly to keep it secure. Follow these requirements to ensure your agency complies with Protective Security Requirements (PSR) for information security.

175. These requirements apply to:

    a. all government information (with or without security classifications)
    b. outsourcing or offshoring your information handling or storage to third parties, such as cloud service providers.

176. 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.

177. The following requirements will help you to protect government information in line with the relevant security classification.

178. This section defines the minimum control and handling requirements. Agencies may apply greater security measures to certain classified information should they deem it appropriate based on the risks that the organisation faces. Refer to the agency's classification and information security policies and procedures for the specific handling requirements for the environment.

Types of security measures for protecting government information

179. 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.

180. Agencies must consider the following minimum security requirements when defining their classification policy and procedures and designing their protective security measures.

General classified information security measures

Creating a registration system

181. Your agency must have a system for controlling and handling government and protectively-marked information.

182. For each document or file, your registration system needs to detail:

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

183. To register media, follow the requirements at 13.2.14 Registering Media (nzism.gcsb.govt.nz).

Maintaining a Classified Document Register

184. You must maintain a Classified Document Register (CDR) for all TOP SECRET and ACCOUNTABLE MATERIAL produced or received within your agency.

185. The CDR should include details of the documents received and all retained copies.

186. It's good practice to maintain a register for SECRET information. You can also use CDRs for documents with lower classifications when necessary for risk mitigation.

187. With due care, your CDR should rarely need to be protectively marked. When it is necessary, mark your CDR on its own merits — not according to the protective markings of the documents it records (unless the title of a document in your CDR is protectively marked, which should be rare).

188. If the volume of correspondence justifies it, use separate registers for each security classification and inwards and outwards correspondence.

Auditing hardcopies

189. Your agency must develop a system for auditing hardcopy information that has protective markings. Audit requirements for ICT systems and equipment are defined in the NZISM.

Using a receipt process to increase security

190. Consider having a receipt process for when protectively-marked information or equipment is delivered to your agency. The benefits include being able to:

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

191. Any type of receipt mechanism is suitable, as long as it identifies the document either by reference number or title.

192. 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'.

193. Specify a period on the receipt (for example, 7 days) in which the recipient must sign and returned the receipt.

194. Confirm you've received all expected receipt returns within a month of their due date.

Spot-checking information marked TOP SECRET and ACCOUNTABLE MATERIAL

195. At irregular intervals, conduct or arrange a spot check of a small sample of TOP SECRET and ACCOUNTABLE MATERIAL to ensure it's accounted for, and being handled and stored correctly. The manager responsible for the information should take charge of conducting or arranging spot checks.

196. Your agency should also conduct spot checks on 5 percent of TOP SECRET and ACCOUNTABLE MATERIAL per month.

197. All (100 percent) of your TOP SECRET and ACCOUNTABLE MATERIAL files must be checked within every two-year period.

Recording spot checks

198. Maintain a record of your spot checks. It is good practice to conduct a similar spot check of other protectively-marked files at irregular intervals.

Reporting discrepancies

199. The manager should report any discrepancies to the Chief Security Officer (CSO), Chief Information Security Officer (CISO), or other appropriate authority for investigation. Examples of other authorities that might be appropriate are the Privacy Commissioner, Ombudsman, National Cyber Security Centre (NCSC), or Cert NZ.

200. See PSR information security (protectivesecurity.govt.nz) for more about managing information security incidents.

Controlling access to information

201. 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).

202. 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.

203. The information's protective marking defines a minimum requirement for specific types of access controls that must be in place to protect the information from compromise.

204. Those with the right clearance must be briefed about the significance of the information and any special handling requirements before they are given access to it.

205. See also:

a. 16. Access Control and Passwords (nzism.gcsb.govt.nz)
b. Physical security (PHYSEC) (protectivesecurity.govt.nz).

Limiting access to authorised people

206. Before you grant access to information with a protective marking, check that the person has the right level of security clearance.

207. They must hold a security clearance that is at the same level or higher than the security classification on the information. People who don't have the right clearance must not be given access.

208. Individuals must have a national security clearance administered by the New Zealand Security Intelligence Service (NZSIS) to be able to handle and access information at: CONFIDENTIAL, SECRET, TOP SECRET levels. Refer to the PSR website on Personnel Security for more information.

209. Government agencies may administer their own security clearance process as part of their pre-employment checks for individuals to be authorised to use information at IN-CONFIDENCE, SENSITIVE, and RESTRICTED. These organisations may utilise the Ministry of Justice Criminal Record Check service or the New Zealand Police Vetting Service if they meet the criteria for access to the service. In addition, contractors and suppliers may require non-disclosure agreements or contracts before being given access to classified information.

210. See also:

a. National Security Clearances (protectivesecurity.govt.nz)
b. New Zealand Police Vetting Service (police.govt.nz)
c. Ministry of Justice Criminal Record Check (justice.govt.nz).

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

What is 'need-to-know'?

211. In common practice, the phrase 'need-to-know' is often used as a shorthand explanation of why information cannot be shared, as in 'sorry, that's need to know'.

212. This is an incorrect interpretation. 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.

213. 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.

214. The words 'need-to-know' of themselves have no explanatory power. 'Need-to-know' simply means that there should be a good reason for an individual to have access to information.

Who decides on 'need to know?'

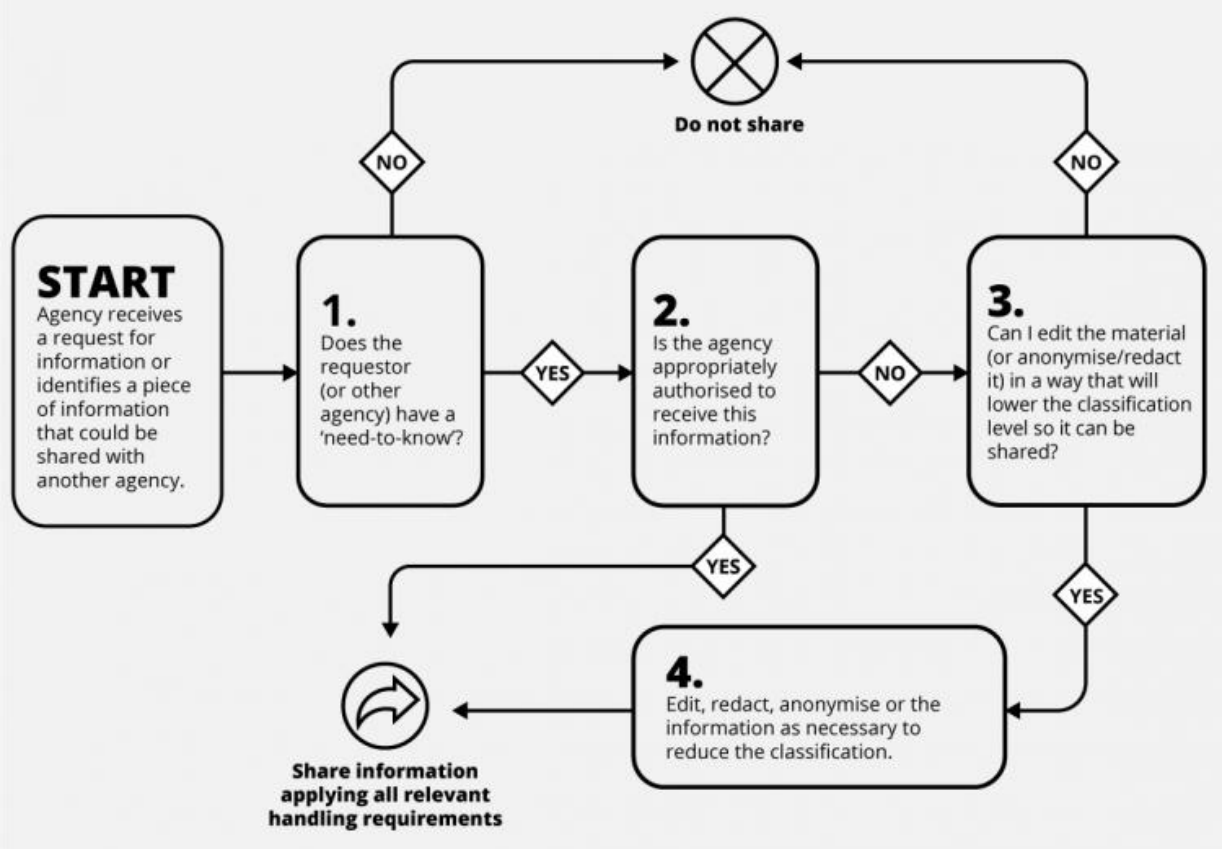
215. Information is 'originator controlled' and the originator and controlling organisation or government decides if the information should have restrictions based on a 'need-to-know'. They will assign an endorsement marking or compartmented marking to indicate the 'need-to-know' compartment which will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

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

216. In most normal circumstances, 'need-to-know' is a two-way process that relies both on the agency 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.

217. Agencies holding information still maintain a responsibility to check whether information should be shared. However, effective information sharing will be better enabled if agencies assume information sharing requests are made in good faith and supported by professional judgement.

Need to know principle flow chart



218. The need-to-know process is a two or three step process that can be applied to any information sharing.

    a. Step 1 confirms whether a 'need-to-know' exists. If there is not a valid reason to access information, it should not be provided. Step 1 confirms whether somebody should receive information.
    b. Step 2 confirms whether the person receiving the information is appropriately authorised to hold it. This might mean that they have the appropriate security clearance and/or systems and locations accredited to manage classified information. In a commercial setting, it might mean confirming a contractor has signed a non-disclosure agreement before sharing business information.
    c. If the decision at Step 2 is 'no', step 3 asks whether information can be provided in a different format (e.g. by removing some more sensitive pieces of information).

Storing and filing information

219. Store government and protectively-marked information in line with Security Zones and NZISM requirements.

Managing electronic information

Storing electronic information

220. 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 New Zealand Information Security Manual (nzism.gcsb.govt.nz). The agency's Chief Information Security Officer (CISO) is responsible for ensuring their systems and that of any supplier to government who holds agency information comply with the NZISM to ensure the information is adequately protected.

221. At a minimum, an ICT system must carry a protective marking equal to the highest security classification of information within it. The agency must consider the value and sensitivity of information within the system as a whole. If the security risks increase when the information is aggregated (combined), the system may need a higher security classification and security measures than the highest classification level of the specific information.

222. An ICT system will be certified to hold government information and data up to a certain classification level. An agency must register their core ICT systems classification level and certification status. 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
    f. operational business systems and databases.

223. ICT systems may be hosted in house or in the cloud and are still required to meet the NZISM minimum standards.

224. An ICT system certified to hold up to TOP SECRET is protected to the highest level and can hold government information at any classification level.

225. User tip: when working with ICT systems, be sure to understand the highest level of classification that the system is certified to hold.

226. You must not store information at higher classifications than the system is certified to hold.

227. For example, if a system is certified to hold up to RESTRICTED, it can only hold information classified at UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE, or RESTRICTED.

Filing electronic information

228. 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.

229. An agency'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.

230. User tip: even when using the same technology (e.g. Microsoft 365), agencies implementation of the security measures and functions may differ. That does not necessarily mean that one agency's system is less secure than another; it only means that the security mechanisms have been implemented slightly differently.

231. Refer to the agency's system user manuals for details on how to protectively mark and handle classified information within each ICT system that you use.

Managing physical files

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

233. Make sure you consider the value and sensitivity of information within a file as a whole. If the security risks increase when the information is aggregated (combined), the file may need a higher security classification and marking.

234. Access, usage and storage or classified information must meet the PSR physical zone requirements.

Adding information to a file

235. 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.

Filing TOP SECRET and SECRET documents

236. Place TOP SECRET and SECRET documents in an appropriate file or cover immediately.

237. The location of at least the TOP SECRET document must then be recorded in the CDR.

Filing information lower than SECRET

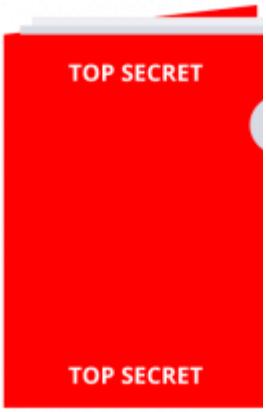
238. If you need to file information marked at levels lower than SECRET, place it in an appropriate file as soon as possible after it is created or received.

Using file references and numbering

239. Your agency should use a file reference and folio number for protectively-marked files, so you can maintain a record of the information held on the file. It is also considered good practice to follow normal filing procedures, such as recording the date and name of the person holding the file.

Using standard colours to make file markings easy to see

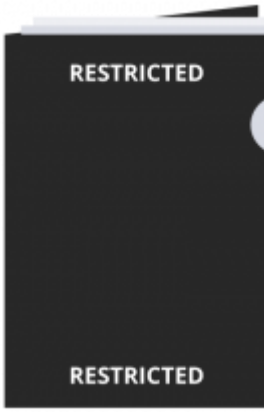
240. The protective markings on files must be clear and easy to distinguish from other markings. If possible, use the standard colours for file covers on your protectively-marked files. (Some agencies might have other requirements that prevent you from using the standard colours).



TOP SECRET
Red

SECRET
Blue

CONFIDENTIAL
Green



RESTRICTED
Black

Using, copying and reproducing information

Using government information

Dealing with verbal information

241. 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.

242. 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.”

243. Ensure that the verbal discussions cannot be overheard by those who are unauthorised to receive the information.

Dealing with virtual meetings

244. ICT systems are certified and accredited to protect information to a maximum classification level.

245. The ICT systems (e.g. telephone and electronic networks, virtual software platforms, and technical infrastructure) used to share and discuss classified information virtually must be accredited to enable sharing of information at the security classification level or higher.

246. Be sure that your 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.

247. See also Storing and filing information (protectivesecurity.govt.nz).

248. User tip: before sharing classified information virtually (e.g. verbally and/or screen sharing), ensure that the systems used are accredited to protect information at the classification level or higher.

249. You must not use or share information at higher classifications than the ICT system is accredited to protect.

250. For example, if an ICT system is certified for sharing up to IN CONFIDENCE information, you cannot dissemination, share, or discuss information at SENSITIVE or higher classifications using that ICT system.

251. Speak to your information security team for more information.

Releasing or changing information with protective markings from another agency

252. If you want to release, share, or transmit information that has a protective marking from another agency, you need to agree the appropriate process with that agency first. This might result in the information being relabelled.

253. You also need the agreement of the originating agency to remove or change a protective marking. If the originating agency doesn’t agree to remove the marking, the information should not be released.

254. If the requirement to release the information is subject to an official information request, an agency may transfer a request to another agency to fulfil the request should the information be held by the originating agency. See the Office of the

Ombudsman (ombudsman.parliament.nz) for more information on official information request transfers.

255. However, the absence of permission to release or acceptance of transfer from the originating agency does not absolve the receiving agency of the obligation to decide on the request. The agency should use the tools provided in the guidance to assess the harm of disclosure against the public interest. This does not prevent the agency from consulting other interested parties before making the decision.

256. See also Security classifications for information from foreign governments.

Copying and transmitting

Copying and using photocopiers

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

258. To make copies of protectively-marked information with a copy number, you must get permission from the originator or originating organisation (the person or organisation that created the information). However, it's better to ask the originator to supply any additional copies that you or your organisation need.

259. If the originator gives permission to make copies, let them know how many copies you intend to distribute. The originator will then tell you which copy numbers you need to mark on your copies.

260. Your agency should develop a policy for use of photocopiers, fax machines and similar devices. Devices used to copy and transmit protectively-marked documents come with risks which you must understand and manage.

261. Photocopiers, fax machines and similar devices, known as multi-function devices (MFDs) may:

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

Reducing risks when you copy and transmit protected information

262. Take the following steps to reduce risks.

    a. Put approved devices in an area where you can observe all copying and transmitting activity.
    b. Make sure a designated person stays near the device until all activity is finished.
    c. Make sure documents are removed from the device as soon as activity is over.

Devices you can't use for copying and transmitting

263. If a device is connected to your ICT system and a document has a higher protective marking than your ICT system, you can't use the device to copy or transmit that document.

264. You also can't copy or transmit a protected document using a device connected to a public network, or a fax machine (unless that information is protected in line with the 11. Communications systems and devices (nzism.gcsb.govt.nz)).

Transmitting electronic data

265. Protectively-marked data that is imported, exported, or transferred electronically must be protected in line with the 20. Data Management (nzism.gcsb.govt.nz).

Reproducing protectively-marked information

266. When you reproduce government information, the original protective-marking and handling requirements still applies to all reproduced information. You must protectively mark the reproduced information at the original marking levels or higher.

267. These requirements apply to all government information (with or without security classifications)

268. Follow these requirements to ensure your agency complies with the Protective Security Requirements for information security.

Managing ACCOUNTABLE MATERIAL

269. Once disseminated, ACCOUNTABLE MATERIAL must not be copied or reproduced in any form. If your agency needs more copies, you must request them from the originator.

270. You also need the originator's permission to extract information from ACCOUNTABLE MATERIAL.

271. ACCOUNTABLE MATERIAL must be destroyed under supervision of two officers cleared to the appropriate level who must supervise the removal of the material to the point of destruction, ensure destruction is complete, and sign a destruction certificate.

272. All TOP SECRET information must be made ACCOUNTABLE MATERIAL by default.

Tracking 'Accountable material'

273. ACCOUNTABLE MATERIAL must have a copy number on the front cover, so your agency can keep accurate records and control distribution.

274. Electronic 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. Refer to the NZISM for more information on controls for ACCOUNTABLE MATERIAL.

275. When protectively-marked information is made 'accountable', the person with responsibility for that information must check and certify its safe custody.

Removing, transporting, or receiving information

276. Security measures and policy for physically removing, transferring, or receiving classified information

277. 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.

278. The intended recipient must have the appropriate ‘need-to-know’ and the required level of security clearance before the information is transferred.

279. Your agency should develop a policy based on the minimum measures, as well as policy for information and material too large for the ‘double barrier’ principle.

Removing protectively-marked information from your premises

280. Understand how to protect government information with protective markings when you take it away from your premises.

281. These requirements apply to all government information (with or without security classifications).

282. Follow these requirements to ensure your agency complies with the Protective Security Requirements for information security.

Putting policies and processes in place

283. If your agency wants to take (remove) protectively-marked information from your premises, you must have policies and processes in place to ensure it’s protected. You might want to take protected information to another agency or workplace for a meeting or to work from home.

284. However, protected information should only be removed from your premises when:

    a. there is a definite need

b. the right level of protection can be maintained en route and at the destination.

Policy for TOP SECRET information

285. You must not remove 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).

Removing protected information within New Zealand

286. Before anyone in your agency takes protectively-marked information from secure or authorised work areas, they must have approval.

Authorising removals

287. Your agency decides who can authorise removals. However, it should be the manager or equivalent person responsible for the information who gives approval.

288. 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.

289. Make sure you keep a record of all removals at TOP SECRET and SECRET levels.

Carrying protectively-marked information securely — briefcases and satchels

290. Your agency should use NZSIS approved briefcases and satchels that are suitable for carrying protectively-marked information. Please contact the PSR team for details.

291. When protectively-marked information is transported outside your agency in an approved briefcase or satchel, you must place it in an opaque envelope within the briefcase.

292. The briefcase or satchel must be:

    a. locked at all times
    b. kept under the personal protection of the custodian.

293. To prevent keys being copied or locks being manipulated:

    a. do not leave the keys in the lock when left in unsecured areas
    b. lock the briefcase or satchel, even when it is empty.

Protecting electronic media

294. You must protect electronic media, such as laptops, CDs, and USBs, used to process protectively-marked information to the same degree as paper-based materials.

295. The level of protection must be equivalent to the highest level of protectively-marked information ever placed on the media until it is sanitised.

Working away from the office or off-site

296. For regular and long-term arrangements for people working away from the office:

    a. follow the security requirements in Working away from the office
    b. refer to Working Off-Site (nzism.gcsb.govt.nz).

297. Sometimes you might need arrange for information to be transferred to a regional or branch office rather than allowing it to be taken to a place where you can't guarantee its security. For example, keeping protected information in a hotel room overnight might not be secure enough in some cases.

Taking protected information outside New Zealand

298. Take special care when your agency plans to take protectively-marked information overseas. It can be exposed to far greater risks, so more security measures are necessary.

299. Read Travelling overseas on business before you authorise any of your people to transmit or handle protectively-marked information outside New Zealand.

Checking with the Ministry of Foreign Affairs and Trade

300. The international Diplomatic Safe Hand Courier Service is administered on behalf of the New Zealand Government by the Ministry of Foreign Affairs and Trade (MFAT) under Articles 27 and 40 of the Vienna Convention of Diplomatic Relations (1961) for the secure transportation of official material classified CONFIDENTIAL or above. The MFAT diplomatic courier network facilitates the secure, routine delivery of classified consignments worldwide. This is the preferred means of transporting all classified information outside of New Zealand. MFAT can provide additional details to any agencies wishing to utilise the Diplomatic Safe Hand Courier Service.

301. If using the Diplomatic Safe Hand Courier Service is not practical, your Chief Security Officer should contact MFAT to discuss alternative arrangements.

Preparing protectively-marked information for transport

302. You must use security measures to protect marked information when it is in transit.

303. 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.

304. Security methods can be used together to create tighter security. For instance:

    a. using an inner and outer envelope — double enveloping
    b. combining an inner barrier with an outer barrier — the ‘double barrier’ method.

305. Whichever combination you use, the inner barrier must be tamper evident and the outer barrier must obscure the nature of the information being transferred.

Addressing information correctly

306. Address protectively-marked information to a specific position, appointment, or named individual.

307. Make sure the addressee and alternative have the required level of security clearance.

308. Specify the intended recipient's name, designation, and full street address.

309. Do not send protectively-marked information to a post office box.

310. For TOP SECRET information, you must provide an alternative individual or appointment. You should also do that for protectively-marked information classified below TOP SECRET.

Transporting information within your office

311. You can transport protectively-marked information within a single location without any coverings, such as envelopes, when:

    a. the information is transported directly between staff who have the appropriate level of clearance to access it and the need-to-know
    b. there is no opportunity for unauthorised people to view the information.

312. If there is a risk that an unauthorised person could view the information, it must be covered.

Double enveloping

313. You must use a double barrier to transport protectively-marked documents securely outside your agency.

314. Double enveloping is used to help protect the need-to-know principle when you transport protectively-marked information and ACCOUNTABLE MATERIAL.

315. Double enveloping provides evidence of tampering. As the name suggests, double enveloping consists of placing protectively-marked information in two sealed envelopes.

316. Your agency must use double enveloping for all information classified as CONFIDENTIAL, SECRET and TOP SECRET when delivering by hand or using an NZSIS-endorsed courier.

317. Use double enveloping at your discretion for information classified as IN-CONFIDENCE, SENSITIVE or RESTRICTED. Use your security risk management plan to inform decisions.

318. SENSITIVE and RESTRICTED information or material must be double enveloped when it is sent by post or commercial courier.

Including receipts

319. Double enveloping must be used along with receipts that:

    a. are enclosed with the protectively-marked documents

b. identify the date and time of dispatch, and the dispatching officer's name
c. have a unique identifying number.

Getting the outer envelope right

320. Use the outer envelope in a similar way to normal mail envelopes. It gives protection to the inner envelope.

321. The outer envelope must not:

a. display the protective markings of the document
b. use tamper-evident seals.

322. The outer envelope must display:

a. the physical address of the recipient
b. a distinct reference number (this may be the receipt number if the envelopes are not individually numbered)
c. the name and signature of the dispatching officer
d. the date of dispatch.

Getting the inner envelope right

323. The inner envelope is used to give evidence of tampering.

324. The inner envelope should:

a. display the protective markings at the top and bottom, and front and back of the envelope
b. be sealed with an NZSIS-approved tamper-evident seal in such a way that covert entry to the envelope is countered.

Using other envelope methods

325. Some single-use envelopes have been approved by the NZSIS for use:

a. as an inner envelope
b. as an outer envelope when used to enclose several inner envelopes where initial delivery will be to a registry or similar.

326. Multi-use satchels may also be used in some circumstances. Please contact the Protective Security Requirements team for details, as the Approved Products List is classified information.

Methods for transporting protected information

327. Your agency should choose the transport method that best achieves the safe transport of protected information.

Using the ‘Safe hand’ method

328. The ‘safe hand’ method is when information with protective markings is despatched to the addressee in the care of an authorised officer, or succession of authorised officers, who are responsible for its carriage and safekeeping.

329. At each handover, a receipt is obtained showing at least:

    a. the identification number of the package
    b. the time and date of the handover
    c. the name and signature of the recipient.

330. The purpose of sending an article using safe hand is to establish an audit trail that allows the sender to receive confirmation that the addressee received the information.

331. To send information using the safe hand method:

    a. enclose it in a double barrier (double envelope it)
    b. give it a unique identification number (usually the receipt number)
    c. place a two-part receipt in the inner envelope with the information — the addressee keeps one portion and signs it and then returns the other portion to the sender
    d. ensure some form of record or receipt system accompanies the package, so that every handover is documented
    e. transport the information in an approved briefcase or mailbag
    f. ensure the information is not be left unattended, except when placed in the cargo compartment of an aircraft.

Using commercial couriers or postal services

332. Your agency can send material classified up to and including RESTRICTED by post or commercial courier within New Zealand.

333. Items classified SENSITIVE or RESTRICTED must be double enveloped.

334. When no authorised messenger or safe-hand courier service exists, your agency can allow material classified CONFIDENTIAL to be carried by signature-required commercial courier or registered post within New Zealand. This method can be used when:

    a. delivery by safe hand can’t be done within 15 minutes (by foot or vehicle)
    b. the sending and receiving agencies have an agreement on the use of commercial couriers for the carriage of CONFIDENTIAL material
    c. arrangements have been made to ensure the receiving agency is able to accept the information at the expected delivery time.

335. Only commercial couriers that have been approved by the NZSIS must be used to carry SECRET material. Your CSO can request details on the requirements and approval process from the NZSIS.

General guidelines

a. Receipts: All CONFIDENTIAL or SECRET information sent via commercial courier or postal agency must be accompanied by a receipt. The receipt must be signed by the receiving agency and returned to the sending agency.
b. Packaging: For carriage by commercial courier, the courier satchel itself when opaque can stand as the outer envelope. Envelopes and wrappings need to be robust to stand up to the wear and tear of transit.
c. Dispatch and delivery: Do not leave protectively-marked information unattended while awaiting pick-up by courier.

336. Don't dispatch protectively-marked information before weekends or public holidays unless the addressee is able to receive it the following day and secure it appropriately.

337. Check your delivery documentation to ensure items arrive within expected timeframes.

338. If there has been an undue delay or there is any sign of tampering, both the sending and receiving CSOs should be notified.

When you can't use a courier or postal agency

339. TOP SECRET material and material with a compartmented marking must not be carried by a commercial courier or postal agency.

340. Special handling requirements that apply to information carrying endorsement markings may also preclude the use of a commercial courier.

341. Information marked with the New Zealand Eyes Only (NZEO) endorsement marking must be transported according to its level of security classification.

342. The requirements for other endorsement markings are established by the controlling agency.

Dealing with bulky material

343. Generally, when the size and weight of material means it can't be moved using the safe hand method or commercial couriers, you need to take special precautions to ensure the material is not compromised, lost, or damaged in transit.

344. Seek advice from your CSO. Your CSO may, in turn, get advice from the NZSIS.

Dealing with high-risk unclassified material

345. If you need to transport valuable material, such as artwork or money, to another agency, you can use commercial courier services.

346. However, take care to assess the courier service first. Make sure it is legitimate, reliable, and can offer the right level of protection for the risks you've identified.

347. You also need to meet any legislative requirements that apply to your material.

348. Whenever possible, avoid drawing attention to the specific nature of the material being moved.

349. Extra security steps might be necessary in some circumstances. Steps such as:

    a. sealing the material
    b. security clearing the employees of the courier service
    c. arranging a security or police escort.

Receiving hard copies

350. Before you allow anyone in your agency to receive hard copies of protectively-marked information, make sure they are aware of their responsibilities and, when necessary, hold the appropriate security clearance.

351. 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.

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

353. 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.

354. 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.

355. 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.

356. If your agency keeps a register for protectively-marked documents, make sure the information is registered.

Destroying classified information

357. Use approved procedures for destroying ICT media and information with protective markings.

358. These requirements apply to all government information and assets that are protectively marked.

359. Follow these requirements to ensure your agency complies with the Protective Security Requirements for information security.

Getting advice and setting policy

360. Your chief security officer (CSO) can seek advice from the NZSIS about approved methods for routine or emergency destruction of protectively-marked information.

361. Your agency should have a policy for destroying government information without protective markings — a policy that is in line with your security risk management plan.

362. You 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.

363. 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.

Disposal and destruction of classified information

364. The disposal of public records must be in line with the Public Records Act 2005, with a current disposal authority issued by Archives New Zealand. Disposal could include either the transfer of records to Archives New Zealand or their destruction.

365. Contact Archives New Zealand for more information.

Destruction methods

366. The following are the usual methods of destruction of protectively-marked information.

    a. Pulping — transforming mass to a given size determined by a removable screen.
    b. Burning — burning in line with relevant environment protection restrictions.
    c. Pulverisation — using hammermills with rotating steel hammers to pulverise the material.

d. Disintegration — using blades to cut and gradually reduce the waste particle to a given size determined by a removable screen.
e. Shredding — using strip-shredders and crosscut shredders. Only crosscut.
f. shredders are NZSIS-approved for protectively-marked information.

367. For advice on equipment for destroying protected information, go to Retire information and assets securely.

Using the shredding method

368. When the destruction method is shredding, you must use the correct grade of shredder for the security classification on the information.

369. The shredder must be approved by the NZSIS.

    a. TOP SECRET information — grade 5 crosscut shredder
        i. Information with compartmented markings — grade 5 crosscut shredder.
    b. CONFIDENTIAL or SECRET — grade 4 crosscut shredder
        i. Information up to and including RESTRICTED — grade 3 crosscut shredder.

Destroying microfiche and other photographic material

370. Protectively-marked microfiche and other photographic material must be destroyed using NZSIS-approved equipment or processes.

Contracting out the destruction of hard-copy material

371. Base any decision on contracting out the destruction of protected material on sound risk management.

372. Here are some factors to consider.

    a. How does the company transport information?
    b. What are their procedures?
    c. How secure are their containers?
    d. How secure is their facility?
    e. What equipment do they use?
    f. What is the result of their destruction process? (For example, the resultant particle size of the destroyed material).

373. Remember that classified waste bags and bins are not security containers. Therefore, they must receive appropriate protection before they are collected. Classified waste bags and bins need to be stored according to the highest level of protectively-marked information they contain.

Getting approval to use a contractor

374. Before your agency 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.

375. Your agency 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.

376. 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. agency representatives with the right level of security clearance must escort the waste and witness its destruction
    e. the destruction company staff must have a security clearance to the highest level of the protectively-marked information being transported and destroyed.

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

Destroying ICT media and equipment

378. ICT media and equipment must be destroyed in line with these two sections of the NZISM:

    a. 12.6 Product Sanitation and Disposal (nzism.gcsb.govt.nz)
    b. 13. Media Management Decommissioning and Disposal (nzism.gcsb.govt.nz).

Transporting sensitive items for destruction

379. For information on securely transporting sensitive information or assets for destruction, please see Securely transporting sensitive items (protectivesecurity.govt.nz).

Managing outsourcing and offshoring arrangements

380. If you're considering outsourcing functions, services, or capabilities to third parties inside or outside of New Zealand, make sure you understand the value, classification, and risks of the information that suppliers and their sub-contractors will have access to.

381. Your agency must follow the outsourcing and offshoring Information Security guidelines and policies. Please see Outsourcing, offshoring and supply chains (protectivesecurity.govt.nz).

Guidance for specific information types

Security classifications for Cabinet documents

382. This section covers Cabinet documents, such as Cabinet and Cabinet committee agendas, papers, minutes, and memos.

383. Documents that Cabinet uses to formulate policy and make decisions require special protective measures.

384. Cabinet documents, unlike other government information, belong to the governments that create them. They're integral to the process by which governments make decisions and they constitute the record of those decisions.

385. Any unauthorised disclosure damages the openness and frankness of discussions in the Cabinet room and impedes the process of good government.

386. The minimum protective marking for Cabinet papers is IN-CONFIDENCE. Higher security classifications should be used if appropriate.

387. To ensure a paper receives the right level of protection, the originating agency (or Minister's office) is responsible applying a security classification to a Cabinet submission.

388. If your agency submits a Cabinet paper without a security classification or with an inappropriate classification, the Cabinet Office will assign the correct security classification in consultation with the relevant Minister's office.

389. When your agency needs to identify special care requirements for Cabinet papers, you should apply an endorsement marking.

390. Endorsement markings used for Cabinet papers include:

    a. BUDGET: proposed or actual measures for the Budget before their announcement
    b. COMMERCIAL: sensitive commercial processes, negotiations, or affairs
    c. STAFF: reference to names or identifiable individuals
    d. SPECIAL HANDING REQUIRED: specific handling requirements apply.

391. Very little information needs the endorsement marking SPECIAL HANDLING REQUIRED and it should be used sparingly.

392. This endorsement marking is specific to Cabinet papers. It may be used with the SENSITIVE security classification if the material in the paper is assessed as highly sensitive in nature and needing additional protection.

More advice on classifying and handling Cabinet material

393. Department of the Prime Minister and Cabinet (DPMC) is the key source for advice on Cabinet processes and material.

    a. CabGuide (dpmc.govt.nz)
    b. Secure handling of Cabinet material (dpmc.govt.nz).

Security classifications for information from foreign governments

394. This section covers applying security classifications to information from foreign governments.

395. 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.

Reciprocal protection under bilateral security agreements

396. Bilateral security agreements can include reciprocal protection for the exchange of protectively-marked information. In such cases, apply the equivalent New Zealand security classification marking. Make sure the protection is equivalent to, but not less than, that required by the government providing the information.

Releasing information from foreign governments

397. Under the OIA, the agency 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 agency on behalf of an government inquiry.

398. Under bilateral agreements, you must get permission before you release information owned or controlled by foreign governments. You should obtain their written approval.

399. However, the absence of permission from another party to release information does not absolve an agency from its obligations under the respective Act.

400. The responding agency must 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.

401. See also:

    a. How to declassify information.

Marking information when there are no bilateral security agreements

402. Consult the NZSIS for help to apply the correct security marking to protectively-marked information you receive from another country — a country New Zealand doesn't have a bilateral security agreement with.

Appendices

2022 Security Classification System policy and requirements

Policy overview

403. This policy describes the Classification System – New Zealand government's administrative system for the appropriate classification and handling of government information. It is not a statutory scheme but operates within the framework of domestic legislation.

404. This Government Security Classification System Policy 2022 and supporting guidance came into force on 1 July 2022. Adoption of this policy by mandated agencies is expected to be completed within 2 to 3 years.

The Classification System policy principles

405. A foundational objective of the Classification System is to encourage and support partnership and collaboration.

406. The spirit of partnership and goodwill envisaged by Te Tiriti o Waitangi is encouraged and supported in how government information is made available, handled, shared and protected. People work together and are inclusive in the spirit of 'mahi tahi'. This principle contributes to learning, growth, and innovation of the Classification System to meet the ongoing needs of all New Zealanders.

407. The Classification System policy is based on these principles.

    a. Organisational accountability
    b. Personal responsibility
    c. Information-sharing
    d. Information declassification

Principle 1: Organisational Accountability

408. New Zealand government agencies who handle government information must establish the conditions that enable people to handle government information correctly and safely.

409. Agency 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 to encourage desired behaviour.

Policy to support organisational accountability

410. **Policy Statement** – Agency 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.

411. The following requirements should be considered when establishing classification policies and procedures.

    a. **Resource and invest** – Agency 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 accordance with all relevant legislation, the Classification System, and regulatory requirements, including any international agreements and obligations. Agencies 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), agencies 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. Agencies must consider the public right to government information and define how they will meet these obligations within their organizational 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. Agencies' 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. Agencies' 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** – Agency 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 agency'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), Agency 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.

Principle 2: Personal responsibility

412. 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.

Policy to support personal responsibility

413. **Policy Statement** – 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.

414. The following requirements should be considered when taking 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 authorization 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** – 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. Agencies should encourage a no blame culture that focuses on learning and improving classification and handling decisions over time.

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

    a. hide violations of law, inefficiency, or administrative error
    b. prevent embarrassment to an individual, organisation, agency, or the government
    c. restrain competition
    d. prevent or delay the release of information that does not need protection in the public interest.

Principle 3: Information-sharing

416. 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.

Policy to support information-sharing

417. **Policy Statement** – Agency 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 agency and with other trusted partners. People are supported and empowered to achieve decision-useful sharing appropriately and safely.

418. The following requirements should be considered when establishing organisational information-sharing policies and procedures.

    a. **Stakeholders' needs** – Agencies 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. Agencies should look beyond their common information-sharing partners including other sector government organisations, international partners, local government, civil defence, hapū, iwi, and local communities. Agencies

must work collaboratively to understand stakeholder needs and what decision-useful information-sharing looks like.

b. **Legislative requirements** – Agencies 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** – Agencies 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, agencies should prioritise investment in removing those barriers where possible.
d. **Use of information-sharing instruments** – When appropriate, agencies 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** – Agencies 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.

Principle 4: Information declassification

419. 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.

Policy to support information declassification

420. **Policy Statement** – Agency 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.

421. The following requirements should be considered when establishing organisational declassification policies and procedures:

    a. **Understanding classified information holdings** – To inform the design of their declassification policy and criteria, Agencies must have a clear

understanding of their classified information holdings as part of their obligations under the Public Records Act 2005 and the Information and Records Management Standard.

b. **Declassification policy** – Agencies that hold 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, decision makers need to 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). This 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** – Agencies 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** – Agencies must appropriately resource and establish a regular programme for declassifying government information in line with their policy and priorities. Agencies must report transparently on the progress, results, and expected value that the programme delivered.

422. See also: How to manage your information (archives.govt.nz).

Legislation requirements

423. Under section 14 of the Bill of Rights Act 1990, everyone has the right to seek, receive, and impart information. As the government holds information that has the potential to harm national or personal interest and security of the public, constraints on this right have been enacted by legislation.

424. The main pieces of legislation that govern the collection, disclosure and use of government information are the Official Information Act 1982 (OIA), and the

Privacy Act 2020. The OIA requires that information is made available on request unless there are specific grounds for refusal. The Privacy Act provides a right of access to an individual's personal information about themselves. It also protects against other infringements on the right to privacy including unjustified collection, use and disclosure of personal information.

425. Outside of requests from the public, there is also legislation that governs the life-cycle of government information. This includes the length of time it can be held, where it is held, how it is disposed of, what it may be used for while held by the government, and the standards to which these activities must be met.

426. New Zealand Public Service organisations and third parties that handle government information must consider all of the legal requirements to make available, manage, and protect government information. They do this under relevant legislation, cabinet directives, strategies, and standards such as:

    a. Official Information Act 1982 (OIA)
    b. Local Government Official Information and Meetings Act 1987 (LGOIMA)
    c. Public Records Act 2005 (PRA)
    d. Privacy Act 2020 (Privacy)
    e. Public Service Act 2020 (PSA)
    f. Declaration on Open and Transparent Government [CAB(11)29/12] (OTG)
    g. Information and Records Management Standard (IRMS)
    h. Protective Security Requirements [CAB (14) 39/38] (PSR).

427. If legislative or regulatory requirements require higher security measures than the minimum requirements in the classification system, apply the legislated or regulated measures.

Official Information Act 1982

428. The OIA provides a statutory framework for processing requests for official information. The OIA generally applies to all information held by government agencies, subject to specific exceptions.

429. The Classification System sits alongside the OIA as an added protective measure with specific emphasis on how certain government information must be handled.

430. The purpose of the OIA is to increase the availability of information and protect information in the public interest. Sections 6, 7, 9, and 10 provide grounds for refusing requests for official information, based on the need to prevent specified harms arising from the disclosure of the requested information. Only those harms recognised by the OIA justify protection – otherwise there is no basis for withholding the information – irrespective of its classification.

431. User tip: sections 6 and 7 provide conclusive grounds for withholding official information, relating to national interest and safety. Section 9 provides justification

for withholding official information unless there is an overriding public interest in release of the information.

432. If compromise of government information would create harm in any of the following groupings, there may be justification to withhold the information.

    a. Defence or security of New Zealand, Cook Islands, Niue, Tokelau, the Ross Dependency or its allies.
    b. International relations of New Zealand, Cook Islands, or Niue.
    c. Maintenance of law and order including crime prevention, law enforcement, and right to fair trial.
    d. Personal harm to members of the public including their health, safety, dignity, liberty, financial status, commercial position, assets, privacy, and identity.
    e. New Zealand economy or economic interest.
    f. Ministers and public service organisations operations including its commercial activities and negotiations.
    g. Maintenance of legal privilege.
    h. Maintenance of constitutional conventions including confidentiality of communications by or with Sovereign or her representatives, confidentiality of advice by Ministers of the Crown and officials, political neutrality, and ministerial responsibility.
    i. Maintenance of the effective conduct of public affairs including the ability to provide free and frank expression of opinions and protections from improper pressure or harassment.
    j. Supply of information provided in confidence where it is in the public interest that information should continue to be supplied or release of it would damage public interest.

433. See also Official Information Act 1982 (legislation.govt.nz).

Privacy Act 2020

434. The Privacy Act 2020 provides the legislative framework for access and protection of an individual's own personal information. (Personal information is a subset of official information. Requests for personal information about third parties are dealt with under the OIA.) The Privacy Act governs all personal information, including information held by public and private agencies. The Privacy Act has thirteen principles that businesses and organisations must follow when collecting, using, and storing personal information. The principles are designed to ensure personal information is protected and respected.

435. Personal information may sit within a classified document. However, as with all other official information, the protective markings on the document do not preclude the personal information from being released if it is requested. The

Privacy Act gives individuals the right to ask any agency (with a few exceptions) for access to the personal information that an agency holds about them. So, if the request is for personal information about the requester, the Privacy Act will apply (even if the information is also official information).

436. The presumption under the Privacy Act is that individuals will be entitled to their information, unless one of the limited withholding grounds set out in the Privacy Act applies.

437. Under the Official Information Act any person or agency may ask a public sector body for any information that agency holds.

438. The presumption under these two Acts is also in favour of releasing information. However, there is a range of withholding grounds which allow public sector agencies to withhold official information.

439. Part 4 of the Privacy act outlines the conditions for the access to, and correction of, personal information. It also provides the grounds for refusing access to personal information.

    a. Security, defence and international relations of New Zealand, Cook Islands, Niue, Tokelau, the Ross dependency, or its allies.
    b. Protection of the Individual.
    c. Trade secrets and Commercial position.
    d. Evaluative Material.
    e. Maintenance of Law and Order.
    f. Unwarranted disclosure of another person's affairs.
    g. Maintenance of legal privilege.

440. There are also Codes of Practice issued by the Privacy Commissioner which modify the application of the Information Privacy Principles for certain sectors or types of information. For example, the Health Information Privacy Code 2020 provides the definition, and specific conditions for the collection, handling and release of health information. A thorough consideration of all legislative requirements regarding personal information is important when responding to a Privacy Act request.

441. See also Privacy Act 2020 (legislation.govt.nz).

Public Records Act 2005

442. The Public Records Act 2005 provides the legislative basis for the creation, disposal and management of government information and public records in all its forms. Through its provisions the PRA supports the accountability of the New Zealand government and provides the public with confidence in the integrity of the records of government.

443. Part 3 (Public Access) of the Act sets out the requirement to determine the access status of those public records which have been transferred to Archives New Zealand or are subject to mandatory transferral (that are 25 years or older). The Act determines that the status for these records should be open access unless there is good reason restrict public access. It also allows for appropriate access conditions to be set to govern access requests to restricted material.

444. See also Public Records Act 2005 (legislation.govt.nz).

How to share information

445. The purpose of this section is to support agencies to establish or improve information sharing practices. It provides relevant information, high level guidance and key messages to support agencies to make improvements within the current policy settings and operating environment.

446. All agencies currently share information, between themselves and the public, in many ways.

447. Information sharing is important. Effective information sharing drives both transparency and public confidence in how public services are delivered and provides agencies with information to deliver better services.

448. Information sharing is complex and dependent on a range of factors. This guidance is written from a security and classification perspective and should be read in conjunction with the other guidance linked to from this material.

449. The guidance:

    a. describes the context of information sharing between agencies
    b. promotes the value of information sharing between agencies and with the public
    c. lays out the policy requirements for information sharing in the New Zealand Government Security Classification System
    d. lays out key legislative requirements that agencies must abide by when sharing information, and references tools and mechanisms that can be used by agencies to enable information sharing.

Application

450. This guidance applies to all government information, regardless of form or format, including speech, documents, and data that the New Zealand government collects, stores, processes, generates, or shares to deliver services and conduct business.

Further information

451. What information can I disclose following a request for official information made under the Official Information Act?

    a. Agency assistance (ombudsman.parliament.nz).

452. What information can I release following a request for personal information made under the Privacy Act?

a. Privacy Act 2020 (privacy.org.nz)

453. How should an agency proactively release official information to the public?

a. Superseded and cancelled circulars (dpmc.govt.nz)

454. How should an agency proactively release historical records that are of interest to the public?

a. How to declassify information

455. How do I know if I need some sort of official agreement to share information, e.g., an Approved Information Sharing Agreement (AISA)?

a. Approved Information Sharing Agreements (privacy.org.nz)

456. How should my organisation manage the ongoing disposal of its records, including deciding which records are of long-term value and will be transferred to Archives New Zealand?

a. Manage information (archives.govt.nz)

457. Where do I go for information about data policy?

a. Data Protection and Use Policy (digital.govt.nz)

458. Why is information shared?

a. Information is shared for a variety of reasons and these affect what type of and how much information should be shared.

Information sharing can improve public services

459. All agencies require information to make decisions and direct their services. This is as true for agencies delivering infrastructure as it is for those delivering services. Information provides the evidence to direct agency outputs, from building new schools to resourcing social services.

460. Effective and appropriate information sharing is important as the information needed for an agency to make robust decisions is often held across numerous / different organisations.

461. In most cases, this can be achieved with aggregated and de-identified information.

Appropriate information sharing supports democratic values

462. Transparency and open government are key issues for democracies. This means that over and above the operational value of sharing information, agencies need to view transparency as a public good.

463. New Zealand has one of the most trusted public sectors in the world. Appropriate information sharing is a key element of transparent and effective government, and

all agencies have a role to play in maintaining and promoting access to government information.

464. Information of this nature is usually shared as a result of either an official request under legislation or through proactive release by the agency.

Better information sharing can improve the safety and security of New Zealand and New Zealanders

465. Information sharing has particular importance for those agencies responsible for public safety and national security issues.

466. Information sharing has many potential benefits and, in the right circumstances, could prevent loss of life. Equally, information sharing on security matters presents challenges, especially relating to the obligations and practices associated with handling more highly classified information.

467. Information of this nature is shared both through established arrangements between agencies and case-by-case sharing as a response to specific incidents.

What does successful sharing of information look like?

468. Success means that information is shared when it can be and protected where it needs to be. Sharing information provides agencies with necessary information through which better public services are delivered. Protecting information means that harm does not result from information being shared inappropriately.

469. Successful information sharing means that information is shared proactively and reactively through well planned arrangements and supported, where necessary, by formal agreements. This includes system to system data feeds as well as contact from one agency to another on specific and sensitive matters.

470. Not all information can or should be shared. All agencies have responsibilities to protect personal information. In addition, agencies working in public safety and national security may face additional requirements to protect information. For example, more highly classified information can only be shared with organisations that have appropriate systems in place. In addition, some agencies may hold information that they are not allowed to share without the permission of the agency that gave it to them (known as 'originator controlled').

Success means agencies can interpret the need-to-know principle

471. The Protective Security Requirements state that 'only people with a proven need-to-know should be granted access to official information'.

472. Need-to-know refers to a 'need to access information based on an operational requirement'. In plain English, if someone needs a piece of information to do their job, they have a need-to-know.

473. However, for several reasons, this does not always mean that they can be given the information.

474. The application of the need-to-know principle is sometimes an impediment to information sharing and the principle is discussed in more detail later.

Success means that agencies proactively look to share information when it would add value to do so

475. As described above, there are clear reasons why some information should not be shared. However, a repeated criticism is that these reasons are over-extended, i.e., used to prevent information sharing unnecessarily and unjustifiably.

476. Collectively, the public service holds large amounts of information that – when appropriately shared – provides insights and informs better services for New Zealand and New Zealanders. If this information is not shared with people who can use it, then it creates no value.

477. Agencies are recommended to take a trust-based approach to information sharing. While need-to-know requirements need to be satisfied, they should not be over-extended.

Success means that agencies only share information that is necessary

478. While sharing information can create value, sharing too much information can also increase risk and cause problems. Sharing more information than necessary makes it more difficult to find and act on the right information. Any information that is shared must also be stored and secured. The more information that is shared, the greater the burden on the agency receiving the information and the greater the risk of that information being inadvertently disclosed.

Success means that agencies consider whether they can achieve information sharing objectives without releasing personal information

479. Information sharing should occur to support specific outcomes, e.g., for an agency to deliver a particular service. Agencies should consider whether these objectives can be met without sharing personal information. Further, if personal information is required, can the same objectives be met if data was anonymized.

480. The underlying principle is that agencies should only share information which is necessary. For example, a health agency might need and request information on the numbers of people receiving a certain treatment and how it was delivered. This information may be held on a database containing personal information about the individuals concerned. In this case, the personal information is irrelevant to the request and would need to be removed if the database was to be shared.

How is information shared?

481. Information sharing can occur in many ways, e.g. with other public sector agencies, private sector organisations, governments, groups, and/or members of the public.

482. The picture below provides a simple summary of the main ways through which information is shared and the key legislation involved.

Sharing information as required by legislation

483. The NZ Government Classification System Policy says, "Agencies 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."

484. To achieve this, organisations need to ensure that their people understand their obligations to share information and can do so, e.g., have the appropriate training and delegations.

485. While it is not always obvious how valuable a single piece of information is, agencies should ensure no one feels they might be sanctioned for sharing information that they have reasonable grounds to think could prevent harm.

486. In general, wherever there is a threat to life or safety information can be shared. Agencies should have policies and procedures in place in the event that information needs to be shared in these circumstances.

Sharing information under the Privacy Act

487. The Privacy Act 2020 provides the rules in New Zealand for protecting personal information and puts responsibilities on agencies and organizations about how they must do that. The Privacy Act governs how organisations and businesses can collect, store, use and share personal information.

488. There are two main types of Privacy Act requests.

    a. Individuals, or agents acting on their behalf, can request information that is held about themselves (requests under Privacy Principle 6)
    b. Anyone (individuals and organisations) can request an agency or organisation to disclose personal information if they believe that the reasons for disclosure are consistent with the exceptions described in the Act.

489. Whenever information sharing agreements are defined in legislation, these have precedence. **Where another law says you should provide information, you are always able to do so.**

490. Information may also have additional, specific requirements about how it can be managed. For example, health information must be managed according to the Health Information Privacy Code. Further information is available from the Privacy Commissioner.

Sharing information under the Official Information Act

491. The OIA allows New Zealanders to have access to information that enables their participation in government and hold governments and government agencies to account.

492. The OIA allows New Zealand citizens, permanent residents, and anyone who is in New Zealand to request any official information held by government agencies.

493. The principle of availability underpins the whole of the OIA. The OIA explicitly states that:

    a. 'The question whether any official information is to be made available … shall be determined, except where this Act otherwise expressly requires, in accordance with the purposes of this Act and the principle that the information shall be made available unless there is good reason for withholding it (emphasis added)'.

494. The OIA aims to increase the availability of official information (i.e., information held by a government agency) to New Zealanders. Under the Official Information Act information must be made available if requested unless a reason exists under the Act for refusing it.

495. While the OIA does not provide a mechanism for information sharing across Government, its principles provide a common reference point to make decisions about information sharing.

496. Further guidance is available from the Ombudsman.

Sharing information under the Public Records Act (PRA)

497. The purpose of the Public Records Act includes 'the preservation of, and public access to, records of long-term value'.

498. Records may be 'open access' (in which case they are available to the public) or 'restricted access'. Section 43 of the PRA requires the chief executive to categorize all public records in existence for 25 years as either open access or restricted access. Section 44 of the PRA specifies that decisions about access must be made based on whether there are good reasons to restrict public access or if other legislation which requires the records to be restricted.

499. When determining whether information and records should be 'open' or 'restricted', organisations should always begin with an assumption of openness unless there are good reasons to restrict. The PRA covers a range of reasons why access should be restricted including national security and international relations and preventing the disclosure of highly sensitive personal information. Without such reasons, records should be 'open access'. Additionally, in specific circumstances, agencies may choose to allow special access to restricted records.

500. The PRA governs the release of archived information and is not primarily a mechanism for information sharing as described in this guidance. Further information is available from the Chief Archivist.

Other aligned legislation and policy

501. Agencies should understand all legislative requirements they have regarding information sharing, for example by identifying and capturing any legislation and policy that has a specific information sharing requirement. For example, the Department of Corrections lists all of its information sharing obligations on its website[1].

502. General expectations of information sharing are set out in the Declaration on Open and Transparent Government[2]' through which 'the [New Zealand] government commits to actively releasing high value public data'.

---

[1] Information sharing with other government agencies (corrections.govt.nz)
[2] Declaration on Open and Transparent Government (data.govt.nz)

Protective Security Requirements (PSR)

503. The PSR is New Zealand's best practice security policy framework. It sets out government expectations for managing personnel, physical and information security. It details mandatory information security requirements and specific protective security measures to manage the NZ Government Security Classification System and the use, handling, management, and storage of classified material. It is supported by the New Zealand Information Security Manual (NZISM) that is the technical authority for technology systems managing government information. The PSR defines the security classification system for national security information and information received from foreign governments. NZ Government must adhere to any provisions concerning the security of such information referenced in multilateral or bilateral agreements and arrangements to which NZ or an organisation is party. Release of information requires written approval from the relevant foreign government. Further information is available from the PSR website.

Proactive information sharing

504. Under the Public Records Act, information of long-term value will become available at a determined point in time. Proactive release of information takes place when agencies choose to release information before that date. This usually happens through the following mechanisms.

Proactive release of government information

505. This includes the release of government information without any request from the public. Government has set expectations that all agencies take a more proactive approach to releasing government information[3]. For example, this has included guidance on publishing completed OIA requests and strengthening the proactive release of cabinet papers[4].

Declassification of highly classified records

506. Few agencies hold substantial highly classified records. Under the NZ Classification System Policy, such agencies are required to have a policy to lay out how they intend to approach the proactive declassification of this material.

[3] Acting in the spirit of service: official information. Proactive release of official information. State Services Commission (2018)
[4] Cabinet Paper: strengthening proactive release requirements (September 2018)

507. The intent of a declassification programme would normally be to release information to the public, i.e., so that it is now unclassified. The principles of the OIA provide clear guidance on whether information would be releasable.

Reclassification of classified information to enable better information sharing

508. When information is highly classified and cannot be shared, agencies should think about whether material can be rewritten at a lower classification level to enable information sharing.

509. Sharing information in these ways requires consideration of how the information is moved, i.e., from a higher classified system to a lower classified system; and who it will be seen by, i.e., between security clearance holder levels and non-security clearance holders. Agencies must ensure that information is moved appropriately and stored where it will only be seen by those who have a need to access the information.

The use of formal information sharing agreements

510. Agencies share information through informal and formal mechanisms. Agencies do not need formal mechanisms to share information within the bounds of the OIA, Privacy Act and other legislation.

511. Information sharing can take place through, or be facilitated by, the following mechanisms:

    a. *Formal Information sharing under legislation includes Approved Information Sharing Agreements (AISAs).* AISAs are formal agreements created under the Privacy Act that allows personal information to be shared between agencies for the purpose of delivering public services. AISAs can authorise information sharing arrangements which grant exemptions to some of the Information Privacy Principles.
    b. *Agencies may also have memorandums of understanding (MoU) to support information sharing.* MoUs do not give any legal authority to share information but do record organisational commitments to, and arrangements for, sharing information.
    c. *Information sharing between agencies.* This can range from staff from different agencies working together on a joint initiative to an individual asking a colleague in another agency to share a document with them. Where an AISA or MOU is not in place, sharing or releasing of information should follow the principles of the Privacy Act and the OIA.

Do I have to have an approved agreement in place to share information?

512. No. AISAs can improve the extent of information sharing and make it happen more efficiently. Where agencies repeatedly share information with each other, formal agreements can be important to set down the purpose for the information being shared and potentially to make information sharing arrangements more efficient.

Opportunities

Leveraging technology to access data

513. Information sharing is still often seen as one agency sending information to another, e.g. by manually sending out data. Such approaches are potentially slow and do not take advantage of readily available technologies.

514. Some agencies are now considering information access rather than information movement, e.g., by providing ongoing access to systems rather than responding to one off requests. This provides scalable and repeatable access to information by providing secure access to agreed types of information.

515. The potential access to greater volumes of data and personal information requires commensurate attention to how access to such information is controlled.

Stewardship not ownership

516. Stats NZ has established a Data Stewardship Framework for New Zealand. Stewardship is a useful concept to enable data sharing as it considers both the ownership and the use of data. For the most part, agencies do not own data but rather they hold data about New Zealanders on their behalf.

517. When used securely and with New Zealand's trust, data should be seen as a means to provide rich insights, inform decision making and innovation and thereby improve services for New Zealanders.

Assessing the need to share information

518. Before agencies share information, they should know who they should share it with and for what purpose.

519. Information sharing most often occurs between relatively small clusters of agencies who have information sharing agreements that reflect shared operational priorities. For example, the Ministry of Justice, Ministry of Health, Oranga Tamariki and other agencies share information to better enable the safety and wellbeing of children and young people in care.

520. Such arrangements are obviously important and of value. Agencies are also encouraged to consider whether there are broader opportunities to share information with agencies not currently considered today.

521. To do so, agencies should first assess the adequacy of existing information sharing arrangements. This could involve the following steps:

    a. Identify what information you hold and how, when and for what purpose is it collected and used
    b. Identify if there is further information that would enable the agency to deliver its services better
    c. Confirm whether the nature and purpose of any new information sharing is permissible (under legislation and relevant policies)
    d. Do existing arrangements support any changes to information sharing? If not, how do they need to be changed?

522. Effective information sharing should flow in two directions. Agencies may receive information from other agencies in order to deliver their own services most effectively. Conversely, agencies may need to provide information to other agencies.

523. This intent faces a practical difficulty that agencies may not know what information other agencies hold and whether they have an operational requirement (need-to-know) for it.

524. It is highly recommended that agencies carry out the proposed steps in consultation with those agencies they work alongside. This will enable agencies to 'know what they don't know' about what information is available and facilitate a conversation about whether there is a need-to-know.

525. Periodic reviews of information sharing requirements and agreement should be undertaken to identify if opportunities exist for further information sharing and to ensure existing arrangements are still fit for purpose. These reviews should include input from staff with operational as well as policy roles, and keep in mind policy and legal considerations.

Which agencies can drive changes to information sharing?

526. All agencies have a responsibility to consider their information sharing arrangements. However, individual agencies may lack the authority or leverage to influence wider information sharing.

527. Lead agencies (i.e., with sector or multi-agency responsibilities) are better positioned to determine whether information sharing can be improved in their areas of accountability. If it is not, they should drive the development of any agreements necessary to improve and broaden information sharing.

Removing barriers to information sharing

Barriers

528. There are a number of barriers to information sharing. This section identifies a range of key barriers and provides some guidance on how to reduce these. It is acknowledged that some barriers, especially those concerning systems, may not be resolvable in the short term. Where possible, some guidance is provided on how agencies can work within these constraints.

Systems barriers

529. Systems barriers exist when technology prevents or restricts information sharing. For example, SENSITIVE or RESTRICTED information require emails to be encrypted and sent and received on a system that is accredited by GCSB to provide an appropriate level of encryption, such as Secure Government Email (SGE).

530. In addition, some agencies may take different approach to technology which makes it harder for them to share information. For example, one agency may want to share information between systems (e.g., by using APIs) and protected by encryption, while another may want to receive information on a USB drive.

Process and behavioural barriers

531. Information sharing requires clear process and delegations. People may want to share information but not do so if they are unsure about how to do so.

532. Overlaying this, people are often busy in the workplace and may take shortcuts to save time. In some agencies, this can lead to automatic over-classification information rather than conscious assessment. This is even more likely if people are not confident about what they should do.

Cultural barriers

533. In some agencies, organisational culture can hinder information sharing, especially where people are concerned about what might happen to them if information is inadvertently released. This is not limited to the national security sector and requirements to manage highly classified information. Privacy breaches can have a serious impact on all organisations.

Information sharing objectives

534. Enabling information sharing requires barriers to be mitigated at many different levels. This section provides some information sharing objectives and supporting actions.

535. At an organisational level, agencies need to understand what information they hold for what purpose and to understand their information sharing obligations. To make improvement, agencies need to evaluate [ideally with other agencies]

opportunities to improve services through more effective information sharing. This requires:

a. Information sharing agreements to be in place [if necessary].

536. At a people level, people need-to-know who to share information with and how to share it. This requires:

a. Clear operational procedures and delegations for information sharing
b. Staff to be confident in applying these procedures, e.g., by having received suitable training
c. Staff to recognise the value of information sharing.

537. At a cultural level, organisations need to have a culture that actively promotes information sharing. This requires:

a. Policies that reinforce the value of information sharing
b. Aligned communications and leadership from the executive down that promotes information sharing

538. It is naïve to assume that policy and communications are sufficient to drive change. The lived experience for some people working in government is that they continue to feel that if they make a mistake with information sharing, it could be career-limiting or even employment-ending.

539. Agencies need to promote both the value of sharing and the value of protecting information. As much as there is a cost to inappropriately releasing information, there is a cost to inappropriately protecting it.

540. An effective information sharing culture does not over-emphasise either sharing or protection at the expense of the other. Rather, it enables staff to make appropriate decisions when they share information and supports them when they have done so.

Applying the need-to-know principle

541. Only people with a proven need-to-know should be granted access to official information.

542. The principle applies regardless of the classification level of the information and the seniority or position of the person asking for information. For example, medical staff have no need to look at a patient's medical records if they are not involved in their treatment.

543. Need-to-know 'refers to a need to access information based on an operational requirement'. In plain English, if someone needs a piece of information to do their job, they have a need-to-know.

544. This does not always mean that information can be released, and need-to-know requirements must be considered alongside the following factors.

    a. Am I allowed to release the information? An agency may hold originator-controlled information which it either cannot release or must seek the permission of the originator before doing so.
    b. Is the person asking for the information allowed to receive it? For some information, a security clearance is required to view the information. In a commercial setting, it might mean confirming a contractor has signed a non disclosure agreement before sharing business information. Equally, some information can only be shared subject to certain controls, e.g., must be shared on an accredited IT system.
    c. Consider if the information could be shared in an anonymised or de-identified format, if the proposed data contains personal information
    d. Consider if there are any other reasons why the information may not be shareable, for example if a Confidentiality Agreement exists.

545. These questions are not about need-to-know but they may prevent information from being shared.

How do I decide if there is a 'need-to-know?'

546. Agencies holding information still maintain a responsibility to check whether information should be shared, including confirming that there is a need-to-know.

547. Within an agency this can be straightforward as need-to-know may be managed by access control. For example, files about some issues may only be accessible to those staff working on them.

548. It is harder to assess whether someone from an external agency has a need-to-know. The receiver of a request for information may not have much knowledge of the other agency's operations and be unable to assess whether the requestor has an 'operational requirement' or not.

549. The guidance recommends that a trust-based approach is used between agencies. Agencies must take a strict approach to handling instructions, e.g. confirming if the recipient of classified information is suitably cleared.

Information sharing case study

Note: this example is illustrative only.

The Chief Executive of a Government Agency is given a highly classified briefing on a potential terrorist threat to their organisation's staff. The briefing contains a number of signs and suspicious behaviours that their staff should be on the lookout for. Their organisation has limited (or no) capability to handle highly classified information and it is therefore not able to be shared.

In this instance, their staff do not have the security clearances and systems required to receive highly classified information and there is no way to pass the information on.

However, the originators of the information could have been more flexible in how things were classified. For example:

Does the most highly classified information need to be in the briefing at all? If the intent of the information is to inform agencies of a threat and advise them of what they should do, is inclusion of highly classified information necessary? For instance, information about how the intelligence services came about information may need to be highly classified but is not needed to meet the intent of the briefing.

Can the briefing be classified by paragraph? If a document is classified as a whole, then the entire document is necessarily classified at the level of the most highly classified piece of information, even if most of the remaining content would be classified much lower. Classification by paragraph makes it much easier to identify and share parts of a document.

When creating a document, it is important to consider the audience and what the objective of that document is. Can the objective be met by providing information that the audience is able to use?

How to declassify information

550. This section provides guidance to organisations on how to declassify government information. The guidance is for any agency needing information on how to meet the requirements for declassifying government information contained in the New Zealand Government Information Security Classification System (Classification System).

551. Government information is all information, regardless of form or format, from documents through to data.

552. The Classification System is mandatory for use within a prescribed list of mandated government departments, the NZ Police, and the NZ Defence Force [CAB (00) M42/4G/4]. This is aligned with the Cabinet decision in 2014 agreeing which agencies are mandated to follow the Protective Security Requirements (PSR) [CAB (14) 39/38].

553. Other government agencies are encouraged to voluntarily adopt the Classification System as a best practice framework for classifying, handling, and protecting government information.

554. In this guide:

a. General guidance provides general guidance to all agencies on declassification.
b. Declassification principles provides specific guidance for those agencies considering or delivering a programme to proactively declassify classified historical records.

General guidance

What is declassification?

555. Declassification includes reassessing how information is protected and – if appropriate – the release of that information.

556. For agencies that protectively mark information, declassification results in a change to the classification of a document. For example, an agency may receive a request for information that is classified as RESTRICTED. After assessment and applying any redaction to declassify the document to allow its release, the RESTRICTED marking should be struck through and the new classification either stamped or watermarked in the document.

~~RESTRICTED~~ **UNCLASSIFIED**

557. Some agencies do not routinely apply protective markings to information. They still however make equivalent assessments about whether information that was protected can be released, e.g., following an Official Information Act (OIA) request.

Declassification is based on an assessment of harm

558. When assessing whether to release information, agencies should consider whether there is any potential harm in release, as this may provide grounds to withhold information.

559. The OIA defines 'good reasons' for withholding information. If such 'good reasons' for withholding information exist, agencies are required to balance this against any public interest in disclosure as this may outweigh the need to withhold. See Public interest: A guide to the public interest test (ombudsman.parliament.nz).

560. When declassifying, you can use the guidance on how to assess harm of its release: Assess the harm.

561. The declassification assessment does not always result in information becoming unclassified: this is called reclassification

562. The declassification process does not necessarily mean information is made public or that it ends up being unclassified. Declassification reconsiders the original reasons for classifying a document and may result in:

    a. A formerly classified record [or part of it] becoming unclassified
    b. The original classification being maintained
    c. A formerly classified record (or part of it) being reduced in classification (reclassification).

563. The last example typically only applies to agencies who hold more highly classified information. For example, agencies working in the national security sector may create SECRET documents which are unable to be shared with most agencies. Reclassification in this context could allow for some material to be removed in order to create a document that could be classified at a lower level, e.g., RESTRICTED which would allow it to be shared more widely.

564. Agencies should use the Business Impact Levels to assess the harm of disclosing classified information and select the appropriate classification level. Guidance on classification is available at How to classify information.

The information sharing landscape

565. As the picture below shows, information sharing can occur in many ways, all of which may require records to be declassified.

Sharing information under the Official Information Act, Privacy Act, and Public Records Act

566. Official Information Act (OIA) and Privacy Act requests are common for most agencies. The OIA states that, *'information shall be made available unless there is good reason for withholding it'*. If there is a good reason (as defined in the legislation) to withhold information, then it can be withheld. Otherwise, it should be released.

567. The purpose of the Public Records Act (PRA) includes 'the preservation of, and public access to, records of long-term value'. Records that have been transferred to Archives New Zealand or are controlled by an access authority may be 'open access' (in which case they are available to the public) or restricted access.

568. When determining whether information and records should be 'open' or 'restricted', organisations should always begin with an assumption of openness unless there are good reasons to restrict. The PRA covers a range of reasons why access can be restricted including national security and international relations and preventing the disclosure of highly sensitive personal information. Without such reasons, records should be 'open access'.

Proactive information sharing

569. Under the PRA, restricted access information will usually become available at a determined point in time. Proactive release of information takes place when agencies choose to release information before that date. This usually happens through the following mechanisms.

Proactive release of government information

570. This includes the release of government information without any request from the public. Government has set expectations that all agencies take a more proactive approach to releasing government information (see: Acting in the spirit of

service: official information. Proactive release of official information. *State Services Commission (2018)*). For example, this has included guidance on publishing completed OIA requests and strengthening the proactive release of cabinet papers (see: Cabinet Paper: strengthening proactive release requirements *(September 2018);* The next steps in the public release of official information).

Proactive declassification of classified archives (the scope of Section 2 of this guidance)

571. Under the NZ Classification System Policy, agencies are required to have a policy setting out their approach to the proactive declassification of their classified archives.

572. This includes a deliberate process to review and prioritise the release of archived material that is of high public interest and suitable for release. For example, this might include information about New Zealand's involvement in the First World War.

573. Relatively few agencies hold information that is suitable for proactive declassification.

Operational reclassification of classified information to enable better information sharing

574. As described above, reclassification can lower the classification to make it easier to share with other agencies.

575. Sharing information in these ways requires consideration of how the information is moved, i.e., from a higher classified IT system to a lower classified IT system; and who it will be seen by, i.e., between security clearance holder levels and non-security clearance holders. Facilitating information sharing in this context requires policies and procedures to ensure that information is only shared with individuals who have a need to access the information and are authorised to receive it.

576. For more information, see the information sharing guidance at How to share information.

Declassification principles

Many organisations have good reasons to keep some information protected but these reasons will not remain valid forever

577. Nations and agencies have good reasons to keep some information protected. This could include personal information about the public, commercially sensitive information received during a tender or [within a national security context] security information obtained from intelligence partners.

578. However, information usually becomes less sensitive with the passing of time. In most cases, agencies cannot justify keeping the information classified indefinitely.

579. For example, information about the location of New Zealand Defence Force members who are deployed in a conflict zone is likely to be highly classified, given that this information could inform an attack against them. However, the same grounds for the classification may not apply after the conflict has ended.

Citizens have a right to government information

580. The proactive release of information promotes good government, openness and transparency and fosters public trust and confidence in agencies. Public access to government information can be restricted excessively if it is not regularly reassessed.

Policy requirements to declassify under the Classification System

581. The Classification System was updated in July 2022 and lays out the following policy for information declassification. This document provides guidance on how agencies may meet each of the expectations.

PRINCIPLE 4: INFORMATION DECLASSIFICATION

582. Government information must not remain classified indefinitely without being subject to review for declassification in line with the Public Records Act 2005, Information and Records Management Standard, and the organisation's declassification policy. This policy should be made available to the public to improve transparency and accountability of declassification decisions.

Policy Statement

583. Agency heads must establish an organisational declassification policy and procedures in line with the Classification System and relevant legislation including Official Information Act 1982, Public Records Act 2005, Privacy Act 2020, and requirements contained in relevant international agreements or arrangements. The following requirements should be considered when establishing organisational declassification policies and procedures.

584. Understanding classified information holdings: to inform the design of their declassification policy and criteria, Agencies must have a clear understanding of their classified information holdings as part of their obligations under the Public Records Act 2005 and the Information and Records Management Standard.

Declassification policy

585. Agencies that hold 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, review periods, and decisions. This policy should be made available to the public to improve transparency and accountability of declassification decisions.

Declassification criteria

586. Not all information may be suitable for declassification if it is of short-term or low value. Within the classification policy, decision makers need to 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). The 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.

Declassification governance

587. Agencies 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.

Declassification programme

588. Agencies must appropriately resource and establish a regular programme for declassifying government information in line with their policy and priorities. Agencies must report transparently on the progress, results, and expected value that the programme delivered.

Impact on agencies

What do I need to do?

589. For most agencies, the main mechanisms through which information is declassified are official information requests and the proactive release of government information such as OIA responses and Cabinet Papers.

Do I need a declassification programme?

590. Declassification programmes are relevant only to organisations that hold classified historical archives that contain information of public interest.

591. Most classified historical information will not be suitable for release. For example, it would never be in the public interest to release an individual's medical records, which may be held for a long time without any expectation of release. Equally,

some classified holdings may be of no obvious utility or interest to the public and are therefore unsuitable for public release.

592. If an agency holds classified historical information whose release would be of public value, it should have policy and procedure describing its approach to declassifying those archives.

593. Section 2 provides some guidance to those agencies for whom this may be relevant.

Guidance for agencies seeking to implement a declassification programme

Meeting Policy Requirements

594. This section provides some practical advice for agencies who may wish to establish a declassification programme for its classified archives. It includes some practical tips from New Zealand agencies (and international partners) about how to run a successful declassification programme. A templated declassification policy has also been produced which agencies can adapt to suit their own needs.

595. **Policy statement** – Mandated agencies are required to have an organisational policy and procedures for declassification of classified archival information. This need not exist as a standalone policy and declassification requirements may be easier to include within existing information management policies.

596. Relevant policies should include:

    a. A high-level commitment to declassification
    b. Reference to any legislation that needs to be considered
    c. Any principles or values underpinning the policy
    d. High level declassification criteria, i.e., about what sort of information the agency believes should be prioritised for declassification
    e. Requirements for implementation, e.g., on review periods for different types of information
    f. Performance indicators, e.g., on what activity the agency expects to undertake each year
    g. Responsibilities for declassification are clearly defined.
    h. Provision for the policy to be reviewed.

Understanding information holdings and assessing the potential value of proactive declassification

597. Agencies need to understand what classified information they hold, assess its value, and then decide what information should be considered for declassification.

598. As noted, much of an agency's classified holdings will not be suitable for release:

    a. Either, it is of no obvious utility or interest to the public
    b. Or, because it is personal information that should not be released (such as court records).

599. The volume of classified information that could be publicly released will likely far exceed the capacity to assess and declassify it. Agencies prioritise where to focus based on a range of factors, including the level of public interest and the feasibility of declassifying different subjects.

Declassification policy

600. The New Zealand Security Classification System Policy states, 'Agency heads must establish an organisational declassification policy and procedures in line with the Classification System'.

601. This does not mean that agencies must have a separate policy for declassification, only that policy exists that addresses declassification.

602. Agencies can choose whether to have a stand-alone policy for declassification or to incorporate this content into existing policies, e.g., their Information Management policy.

603. Some agencies have asked for guidance on how to develop a declassification policy. The Declassification Policy Template (protectivesecurity.govt.nz) is provided primarily as a starting point for agencies considering establishing their own declassification policy and need guidance.

604. The template is not prescriptive, and agencies should apply their own judgement about whether the content is useful to them or whether declassification requirements are already addressed in other policies.

What topics should be addressed?

605. Agencies can take several approaches to identify themes suitable for declassification, including:

    a. Analysing Official Information Act requests to identify themes of most interest
    b. Engaging with the public, such as through the historical and academic community to determine areas of most interest
    c. Selecting topics of greatest value or scarcity, e.g., Pacific Island records.

Declassification governance

606. Governance arrangements should be proportionate to the size of the declassification programme.

607. Effective declassification involves responsibilities at several layers, from deciding what topics should be addressed to approving the release of information. Who fills those roles must be contextualised for each agency.

Establishing a declassification programme

608. This section provides some practical tips on how agencies might go about delivering a declassification programme. The tips are based on New Zealand experience and that of overseas partners.

Declassification needs people with experience and expertise

609. Declassification decisions are often complex, nuanced and require significant knowledge of an organisation's history. While at one level the task is administrative, declassification decisions rely on expert judgement and substantial organisational experience.

Declassification needs a team

610. Given the level of professional judgement involved, it is unrealistic to expect individuals to draw identical conclusions to each other. Ideally, people should work within a team so that discussions can be discussed collectively and made more consistently.

Advice on where to start

611. To begin with, historical declassification should be targeted against areas of wider utility or interest to the public. Historical declassification is time-consuming and would be largely a waste of effort if applied to topics of limited interest.

612. After having identified topics of public interest, agencies will probably still have a much larger volume of information than they have the resources to declassify.

613. Agencies should therefore include pragmatic considerations about what to declassify. For example, agencies will also find it easier to begin with declassifying older, non-electronic records as relevant artefacts are usually already archived and easier to find.

Corporate services need confidence in the declassification process

614. Various functions in an agency may have an interest in declassification, including legal, risk management, compliance, audit, and others.

615. It is recommended that relevant corporate functions are involved in the development of declassification policy and procedures. Their input on individual records should be by exception and policy should give guidance to where this might be required. For example, the advice of the legal team may be required if items in a record relate to a matter that was subject to a legal process, but one

would not expect the legal team (or other corporate services) to review every document.

How often should agencies declassify?

616. While the choice of when to proactively declassify records is up to the agency, it is preferable to release regularly, i.e., a few times during each year. The reason for this is that some agencies report that if records are only rarely declassified, then people tend to forget (and have to relearn) how decisions were made previously.

617. Where declassification occurs more frequently, organisational memory of the process is usually retained, and subsequent rounds of declassification can become more efficient. This is greatly assisted if the reasons for any key decisions are recorded when files are being declassified.

Who should run a declassification programme?

618. Declassification programmes could be run from several parts of an organisation. However, the process most naturally fits within the responsibilities of a knowledge or information management team.

Do I need to involve other agencies?

619. Agency experience to date has been that topics for declassification tend to be either specific to agencies or of different importance to different agencies. For these reasons, joint-agency declassification programmes (while compelling in theory) are unlikely to be feasible.

620. However, agencies should engage with other agencies if a proposed topic for declassification is likely to have a high impact on them, e.g., result in a large number of OIA requests for another agency, or if they have other reasons for the information to remain classified.

How do I report on the value of the declassification programme?

621. Mandated agencies will provide some information about their declassification programmes through the PSR self-assessment and reporting process. However, this information is not publicly available. It is recommended that the easiest way to report publicly against declassification activities is to include a short description in the agency's Annual Report.

How to adopt the Security Classification System

622. In this section you will find guidance on:

    a. what has changed in the policy and guidance effective 1 July 2022
    b. how to meet the policy principles
    c. how to implement the Classification System in your organisation
    d. how to measure the performance of the Classification System
    e. how to deploy the user training modules.

What has changed in the 2022 Classification System

Why has the Classification System been changed?

623. The Royal Commission of Inquiry (RCOI) into the terrorist attack on Christchurch masjidain made a number of recommendations towards the objective that, 'public sector agencies can and should share information more widely'.

624. In particular, the RCOI referenced the need to classify information correctly and to use the need-to-know principle to enable rather than restrict information sharing.

625. The 2022 changes have not fundamentally changed the Classification System; rather they have introduced a change in emphasis to meet the RCOI recommendations.

What outcomes are sought by the change?

626. By implementing the policy, the following outcomes are sought:

    a. more consistent and effective use of the Classification System through standardized education and training across government.
    b. more purposeful information sharing leading to reduced national security risks and improved government services.
    c. an increase in transparency and public engagement through regular declassification of information.

What has stayed the same?

627. The structure, levels and definitions of the New Zealand Government Information Security Classification System (Classification System) are not changing as a result of this project.

628. For those familiar with the Classification System, changes are mostly about a change in emphasis to promote information sharing. Those with existing

knowledge will not need to learn new rules about how to classify and protect information. However, experienced agencies can use the new plain English guidance aimed to make it easier to classify and protect information.

What are the key Classification System changes?

629. Specifically, the following topics have changed. Review the updated content to determine how your practices may need to change.

Topic	Nature of the change
Classification System Policy	To enable the RCOI recommendations, the new Classification System policy includes four overarching principles and clarifies the requirements and behaviours expected by agencies. This include new principles and policies to support information sharing and declassification. While these changes do not substantively change the Classification System itself, they are designed to encourage some change in how it is applied.
Classification System Resources	There are new or updated Classification System resources for your use including online training modules, FAQs, and other downloadable documents, campaign collateral, and tools.
Secure handling requirements (now under How to protect information)	The secure handling requirements have largely not changed. We have moved them into a new section called 'How to protect information' and created or updated the following sections: • Endorsements for policy and privacy classifications • Quick Guides for all Classification levels.

When do the changes become effective?

630. The policy became effective on 1 July 2022. However, we understand that it will take agencies some time to implement them in their organisation.

PSR mandated agencies

631. PSR mandated agencies will first be assessed against the changes in March 2024. The table below shows the key actions required of PSR-mandated agencies.

632. Agencies will typically begin gathering evidence around November each year to be ready to submit their self-assessment in March the following year. By this assumption, PSR-mandated agencies will need to have made any required changes by the end of October 2023 in order for these to be captured in the March 2024 self-assessment.

July 2022	Release of new policy
July 2022 – March 2023	Agencies agree what maturity level to target for the March 2024 self-assessment. Agencies assess and plan how they will adopt the classification system policy.
March 2023	Agencies report back on their classification improvement plan in PSR self-assessment report.
March 2023 – March 2024	Agencies develop and new policies, processes and guidance required to implement. Nov 2023: • Agencies begin gathering evidence for the self-assessment. • Agencies continue classification improvement plan.
March 2024	First receipt of self-assessment from PSR-mandated agencies.

633. This gives agencies about 16 months to make changes once the new policy is introduced. Agencies will need to make their own assessment about how much change is realistic. For example, an agency may choose to target a 'basic' maturity level initially, if their risks are low and it does have the resources to meet all the requirements of a higher maturity level.

634. Please note, if the agency chooses to target 'basic', they will not 'meet' the mandatory requirement for INFOSEC2 in the November 2023 to March 2024 self-assessment round.

Non PSR mandated agencies

635. Agencies that are not PSR mandated are not required to complete the PSR self-assessment process. However, the PSR guidance and self-assessment requirements do give a clear indication of what best practice looks like.

636. All agencies are encouraged to consider these requirements against their own business needs and to consider what changes they may need to adopt to better manage their protective security.

How to meet the classification principles

How to meet Principle 1: Organisational accountability requirements

637. Principle 1 states that:

    a. New Zealand government agencies that handle government information must establish the conditions that enable people to handle government information correctly and safely.
    b. Agency 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 to encourage desired behaviour.

638. **Policy Statement** – Agency 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.

639. To meet your obligations under Principle 1, organisations need to:

    a. **Have a classification policy**: Review your agency's existing classification policy or establish a new policy. You can use the sample classification policy which can be adapted for your organisation. This policy should include:
        i. Roles responsible for management and support of the Classification System
        ii. Outline the core legislative, regulatory, legal, organisational policy, and partner requirements that governs information creation, security, management, sharing, declassification, and release.
        iii. Define the core policies and principles for classification
        iv. Link to related policies, guidance and standard operating procedures.
    b. **Establish classification procedures**: Review and update your procedures and guidelines for handling government information (including partner information) securely and correctly.
        i. Security classifications and protective marking guidelines
        ii. Partner information guidelines.
    c. **Provide people with regular and ongoing classification training**: Provide your people with timely and ongoing classification training including how to classify it, handle it, share it, and declassify it. This training should form part of your wider information management and security training. Regularly assess how well people understand and can use the Classification System.

d. **Build classification policy requirements into your supplier contracts**: Suppliers and third parties become an extension of your business and broaden your security risks. Build your classification policy requirements into your contracts and require your suppliers to do the same when sub-contracting work to other suppliers. Provide your supplier's staff with regular and ongoing training to ensure they understand how to classify and handle your information securely. Build assurance activities into your supply chain management functions which include evaluation of their compliance with your classification policy.
e. **Undertake regular reviews of classifications**: Information sensitivity will change over the information lifecycle and therefore protective markings should be reviewed to ensure they are still appropriate. Pragmatically, you can perform reviews over the information lifecycle:
    i. The information owner/creator can review while drafting, editing, changing, publishing, or disseminating the information
    ii. A user can review and confirm the classification when using the information and raise any clarification/justification requests to the information owner if they think it is no longer appropriate (including under a request for official information release)
    iii. An information management or security professional can review and audit a random selection of information and record its findings and recommendations to learn and improve capability over time.
    iv. A declassification officer will review historical records as part of the declassification assessment.
f. **Ensure your classification approach is fit for purpose**: Regularly review how well the classification practices are working for your organisation. Plan improvements and report back on your programme.
    i. Assess performance by looking at recent information vulnerability assessments, information compromises, and outcomes from audits by internal staff, the Ombudsman or the Chief Archivist.
    ii. Assess if you have the right resources and investment in classification commensurate with the risks faced by your organisation.
    iii. Plan improvements or changes to classification efforts as part of your protective security improvement programme. This can include changes to roles and responsibilities, policies, procedures and guidance, training and education, or leadership and communication.
    iv. Assess your classification capability as part of your protective security capability maturity assessment. Annually, report back on

the performance of your programme and areas for further investment and improvement.

640. See also:

- Template classification policy (protectivesecurity.govt.nz)
- How to measure the performance of the Classification System
- How to adopt the Classification System
- Supply chain security (protectivesecurity.govt.nz).

How to meet Principle 2: Personal responsibility requirements

641. Principle 2 states that:

    a. 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.

642. **Policy Statement** – 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.

643. To meet your personal responsibility obligations, people working with government information need to:

    a. **Build and keep your classification knowledge and skills up to date**: Attend and participate in available training and education and read guidance materials to ensure you can fully understand and fulfil your obligations for correctly classifying and handling information securely and correctly.
    b. **Become adept at assessing and articulating the harm of information compromise**: 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. Even unclassified information is protected. Each information set will have different sensitivities which will change over time. Use paragraph marking to help you keep track of the parts of information that have greater or lesser sensitivity. Be able to justify the classification decision.
    c. **Set the duration of protective markings**: When you first apply a protective marking to information, try to set a date or event when you will review it for declassification. Base the date or event on an assessment of how long the information will remain sensitive. For example, Budget

papers need high protection before the Budget's release, but not afterwards. Some information may need increased protection because it is under embargo until a specific public policy statement, after which time it becomes public information. On reaching the date or event, the information should be automatically downgraded to a more relevant level of control.

d. **Seek and act on classification learning opportunities**: When using information, don't take the classification or protective marking at face value – do your own risk assessment and seek clarification from the information owner if your assessment differs. Be open to challenge on the information you classify. If you can justify your assessment, you can have a useful conversation on potential harm and risk. Note that information sensitivity will change over time, and it may be time to change the classification. Use these interactions as learning opportunities for both parties; do not look to blame or shame.
e. **Consider the intended audiences who could benefit from the use of the information**: When creating information for use by others, 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.
f. **Don't withhold information inappropriately**: It is not appropriate to use classification or protective marking to withhold information inappropriately such as to:
    i. hide violations of law, inefficiency, or administrative error
    ii. prevent embarrassment to an individual, organisation, agency, or the government
    iii. restrain competition
    iv. prevent or delay the release of information that does not need protection in the public interest.

644. See also:

a. Classification User Handbook (protectivesecurity.govt.nz)
b. How to classify information
c. How to protect information
d. How to share information
e. How to declassify information.

How to meet Principle 3: Information-sharing requirements

645. Principle 3 states that:

a. 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.

646. **Policy Statement** – Agency 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 agency and with other trusted partners. People are supported and empowered to achieve decision-useful sharing appropriately and safely.

647. To meet your obligations under Principle 3 organisations need to:

    a. **Ensure policies reinforce the value of information sharing**: Information sharing is authorised and enabled in many areas and recommend that the value of information sharing is embedded into appropriate policies, e.g. Declassification Policy, Information Sharing agreements, Information Management policies etc. The concept of Information-sharing should be embedded into information management best practice.
    b. **Understand the stakeholders you need to share classified information with**: Agencies should know what information they need to do their job and what information they hold that will help others do their job. From an operational point of view, a lot of information sharing happens already. Assess the following questions:
        i. Are you sharing with everyone you should (inside and outside the organisation)?
        ii. Is the information that is being shared fit for purpose?
        iii. Is the classification appropriate for intended distribution?
    c. **Understand your information-sharing obligations under relevant legislation**: Information is often not shared due to misunderstanding of the relevant legislation and/or fears of acting outside the legislation. While these behaviours are the result of both attitudes and knowledge, agencies should assess whether staff knowledge is accurate and, if not, provide training to address any knowledge gap.
    d. **Identify any barriers to effective information sharing**: Information sharing is a business process that can be influenced by many factors, including culture, people factors, processes and technology. Agencies should identify any specific barriers to information sharing in their own

context. For example, working on culture will not improve information sharing if the underlying need is that there are no agreements in place to share information.

e. **When appropriate, agencies should make appropriate use of available government information-sharing instruments**: Not all information sharing requires formal agreement. However, the delivery of effective public services can be enabled by appropriate agreements, from Memorandums of Understanding to Approved Information Sharing Agreements. An AISA is a legal mechanism that authorises the sharing of information between or within agencies for the purpose of delivering public services. An AISA authorises agreed departures from some of the privacy principles, if there is a clear public policy justification and the privacy risks of doing so are managed appropriately.
f. **Establish policies, procedures and training for sharing classified information**: Effective information sharing requires several things to work. Organisations must adopt and promote it, systems must make it possible, processes must enable it and people must have the skills and motivation to do so.

How to meet Principle 4: Information declassification requirements

648. Principle 4 states that:

a. 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.

649. To meet your obligations under Principle 4 organisations need to:

a. **Understand what classified information your agency holds**: Before writing a declassification policy, agencies need to understand what classified information they hold, how that information is currently scheduled for release and what public value the release of this information would hold.
b. **Have a declassification policy**: You can use the sample declassification policy which can be adapted for your organisation.
c. **Establish declassification criteria**: Agencies need to set declassification criteria that are consistent both with information management standards and with common sense. With regard to information management, this means that agencies need to establish rules and standards for how classified information will be managed and for how long it will be

classified, and for the process of declassification. This ensures that the classification applied to most information will end (or be reassessed) after an agreed time period.

650. Agencies also need to consider the proactive declassification of archived material, i.e. releasing information of high public value before required by policy. Where agencies hold archived classified information of public interest (e.g. relating to key moments in the nation's history), they are encouraged to determine criteria through which these can be released and establish a programme to do so.

    a. **Establish declassification governance**: Agencies must establish an appropriate governance framework for declassification. Governance bodies must: ensure that declassification: delivers value for the public; and, have the organisational experience [and political acumen] to arbitrate declassification decisions when conflicting opinions arise.
    b. **Establish a declassification programme**:
        i. Where appropriate, agencies should appropriately resource and establish a regular programme for declassifying government information in line with their policy and priorities.
        ii. Agencies must report transparently on the progress, results, and expected value that the programme delivers (most likely via their annual report).

651. See also:

- How to declassify information
- Template declassification policy (protectivesecurity.govt.nz)
- Declassification guidance (protectivesecurity.govt.nz).

How to implement the Classification System

What steps should you take?

652. At the highest level, all agencies that use the Classification System should:

    a. familiarise themselves with the policy
    b. assess any gap between the policy requirements and their existing policy and processes
    c. agree any actions required to address that gap.

653. Agencies should also consider whether their culture and ways of working are aligned to the policy's intent. The reasons why information is not shared are often as much cultural as procedural. Some agencies will not be able to make significant change to how they share information without addressing cultural factors that inhibit information sharing.

654. The table below indicates the possible activities, within each area, that agencies should make to adopt the Classification System:

Assess Policy Change	
Assess impact of changes on current protective security policies, procedures, and practices.	The first step for all agencies should be to review the new Classification System policy and assess whether existing policies and procedures are fit for purpose.
Assess gap between current practices and the agency's desired future state.	Agencies need to decide what changes they are going to make in response to the changes. The amount of change should be proportionate and take into consideration current maturity and business need.
Plan (and deliver) work to implement any required changes.	For some agencies, delivering these changes may require a plan and resources to ensure changes are implemented on time.

Assess Behavioural Change	
Assess current culture, especially with regard to information sharing.	Agencies have different tolerances for information sharing and should begin by assessing their current culture towards the sharing of information.
Assess gap between current information sharing culture and desired future information sharing culture.	Agencies need to consider if their current culture enables them to share information in the way they would like to. If it is not, agencies should agree what change they think is necessary.
Confirm leadership is committed to any desired culture change.	Any behavioural change is hard and is unlikely to succeed if led by practitioners alone. If agencies need to make substantive change to embedded ways of working, they will only succeed if this has strong commitment from leaders.
Plan [and deliver] work to implement any required changes.	Agencies need to consider how any behaviour change can be built into their planned work. This may require specialist change management and communications support.

Assess Training Material	
Review and adopt centrally developed Classification	The training modules are designed to be directly adopted. However, agencies may wish to deploy the modules within their own Learning Management

System education and training packages.	Systems, especially as this will give them the capability to record attendance and completion.
Choose whether to adapt and customise training modules and/or develop agency-specific training.	The training modules are designed to be generic. Agencies may feel they can be made more meaningful if they are adapted, for example with more examples that are specific to the agency and with the inclusion of additional information. This will require time and resource from their own Learning and Development teams and security practitioners to develop/update content.
Plan [and deliver] training.	Once training materials are developed, agencies will need to integrate these with their existing training requirements (this may require the content to be adapted).

How to assess and manage the change impacts

655. Some agencies have requested advice on how to introduce change. The need for change management support varies widely between agencies.

656. At the low end, some agencies have asked only for clear guidance and education materials and have all the necessary capability to roll this out themselves.

657. At the high end, some agencies have requested much more specific help with tools, templates and processes.

658. A Change Toolkit (protectivesecurity.govt.nz) has been developed to provide agencies with a reminder of the broad change management steps that any organisation should take to give the best possible chance of success/adoption.

659. It is not intended to be prescriptive or to deliver a comprehensive set of change management tools. The toolkit contains an organisational assessment and communications guidance.

660. The organisational assessment allows agencies to assess their current maturity in using the Classification System, agree their future maturity and identify what high level changes they will need to make. The assessment is specifically targeted at assessing maturity in using the Classification System. The organisational assessment is tailored to classification issues and is applicable to all agencies. This provides an objective basis for agencies to assess their current maturity and assess whether this is adequate.

661. The Communications Guidance provides some support for agencies to consider:

a. what groups of people in their organisation will be affected by changing the classification policy
b. what is the best way to communicate with them
c. what they should feel, think and do after the new policy is rolled out.

662. The communications guidance provides some support for agencies looking for help in how to deliver change. Agencies with specialist resources and capability in delivering change will probably use their own resources and methodology to deliver change.

Implementation roles and capabilities

663. The resource available to support implementation of the classification system policy will vary from organisation to organisation. In general, the more minor the change to existing practice, the less support will be required. For example, small changes to policy can be introduced by practitioners successfully.

664. However, for some agencies to achieve the policy objectives, they may need to confront legacy cultures, systems and processes that have become engrained and often actively resist information sharing. Change of this nature is dependent on leadership, people who are experienced in delivering change and a commitment to stay the course.

665. Failed change initiatives can be costly and often result in the desired change being deprioritised for years to come. It is important that agencies strike a pragmatic balance between what change is desirable and what change is probable to succeed.

666. Depending on the size of the change, you may need people with the following capabilities:

a. classification and information security – for classification and security policies and practice implementation
b. information management – for information sharing and declassification policies and programme implementation
c. learning and development – for classification training adoption, adaptation, and implementation
d. organisation change management – for understanding, planning, and carrying out key communication and change management to drive the culture change needed and measuring how well the change has been achieved.

How to measure the performance of the Classification System

667. Use the Protective Security Requirements assurance and reporting tools below to assess the maturity of your organisation's classification capability alongside your other protective security capabilities.

668. The PSR assurance tools have been updated to include additional maturity indicators related to the Classification System across different capability dimensions. These tools are available to any organisation to measure their performance in the use of the Classification System.

Tool	Usage
Protective Security Capability Maturity Model (July 2022)	The model enables you to assess the maturity of your classification capability alongside your other protective security capabilities and help you to identify how you could develop them further. The model recognises that each organisation has a unique combination of security risks and areas it needs to protect and enables organisations to use a risk-based approach to managing their security risks. The model assesses capability across 12 dimensions and 4 maturity levels. The model is guided by the PSR's mandatory requirements. While the 20 mandatory requirements are 'baseline' objectives, the model helps all types of organisations to set maturity targets based on their own security risk profile. One size does not fit all.
PSR Moderation Framework (July 2022)	Agencies need to provide the underlying evidence to support their self-assessment against the Capability Maturity Model. The evidence is broken down into evidence of policy and processes versus evidence of practice (such as registers, logs, or reports) showing the outcomes of the policy and processes and how they are used to improve on outcomes. The framework can be used by agencies themselves for informal self-assessment or by independent auditors for formal audit of the self-assessment (see the All of Government protective security panel for more information).
PSR Roadmap template	The PSR Roadmap template can be used to capture your organisation's goals and improvement plans across the 20 PSR mandatory requirements.
Self-assessment report template	The report template can be used annually to report back on your organisation's protective security capability and

	improvement plans to agency leaders and directors as well as to government leads. If your organisation is mandated to follow the Protective Security Requirements, this reporting is mandatory and shared with the PSR/GPSL and GCSB/GCISO.
Classification System changes to CMM & Moderation Framework	This provides an overview of the changes specifically related to measuring the performance of the Classification System. Use this guidance to understand what additional capabilities and evidence you will need to demonstrate good practice in the Classification System.

Classification capability is measured under Mandatory Requirement INFOSEC2

669. The Classification System is part of the Protective Security Requirements Mandatory Requirement INFOSEC2.

670. When undertaking your self-assessment against this mandatory requirement in the October 2023 to March 2024 period, you will need to also consider the additional Classification System requirements to determine how well you meet this mandatory requirement.

671. For example, if you previously rated yourself as 'Meets' for INFOSEC2 but as at March 2024, you have not yet put in place all of the additional capability as defined in the July 2022 updates, then the status of your compliance with this mandatory requirement must reduce ('Mostly meets' or lower) as you no do not meet the updated mandatory requirement.

Examples for new Classification capability under the CMM dimensions

672. Below are a couple examples of the Leadership and Culture capabilities you will need to have in place be considered 'Managed'.

Dimension	Capability (Managed)	Examples of Evidence
Monitoring and assurance	• You are auditing and recording the quality of classification decisions • You apply evidence-based performance measures to help track and assess the ongoing success of the information sharing and declassification	• Reporting in outcomes of audit and review of classification • Evidence of business change based on classification audit and review • Process for monitoring classification,

		declassification, information sharing • Audit and review of classification procedures • Chief Archivist and Ombudsman feedback
Culture and behaviours	• Your people regularly review and challenge classification decisions and learn from mistakes • Your people make classification decisions that effectively manage the tension between needing to know (withhold) versus needing to share (open) • You understand all the information you hold, and have systems and mechanisms in place to enable sharing to occur with any appropriate partner (including emergency management, communities, and social services) • Your staff understand the value of information sharing and are formally empowered to share information appropriately where of value to other agencies	• Classification System (including Information sharing and declassification) awareness campaign • Information Sharing Plan • Information Sharing culture survey • Measurement of changes in classification rates, volumes of declassification, decrease in complaints, positive ombudsman reporting

How to deploy user training modules

673. There are five online training modules for the Classification System. These modules are aimed at anyone who creates or handles government information. This includes all employees, contractors, and suppliers to Government.

674. The modules are designed as an introductory course to be given during induction and then as refresher training as required.

675. The modules are available for organisations to use in four ways:

Host modules on agency's learning management system (LMS)

676. We can provide your agency with the LMS enabled SCORM 1.2 and 2004 files. For more information and access to the files, contact the PSR team.

Host modules on agency intranet

677. For agencies who do not have a LMS to host the online training, they can host it from their intranet. Refer to your ICT team for deployment of these files on your intranet. We can provide your agency with website enabled files. For more information and access to the website files, contact the PSR team.

Tailor the modules to specific agency context

678. The modules were developed using Articulate Storyline 360. To tailor the modules, you will need access to Storyline 360 v3.63.27674.0 or higher. We can provide your agency with Storyline files. For more information and access to the Storyline files, contact the PSR team.

Run modules hosted on PSR website

679. For agencies that cannot host the files on an LMS or intranet, they can run the modules direct from this website. Note: Your organisation will not be able to track learning completion or outcomes for each user who accesses these modules via this website.

Module 1: Introduction to classification (protectivesecurity.govt.nz)

Duration: 15 minutes

Audience: All government employees, contractors, and suppliers

In this module we'll provide you with an introduction to the New Zealand Government Information Security Classification System (classification system). By the end of the module, you'll be able to:

- explain the benefits of classification
- explain the consequences of poor classification
- explain what classifications are
- explain what protectives markings are.

Module 2: How to classify information (protectivesecurity.govt.nz)

Duration: 25 minutes

Audience: All government employees, contractors, and suppliers

In this module we'll look at how to classify government information using a harm-based approach.

By the end of the module you'll be able to:

- understand the relationship between harm, impact and classification
- describe the different types of impact
- assess the level of harm and impact that compromise of information could have
- classify information based on its impact.

Module 3: How to protect information (protectivesecurity.govt.nz)

Duration: 15 minutes

Audience: All government employees, contractors, and suppliers

On completion of this module you will understand:

- how to protectively mark information
- who can handle classified information
- how to securely handle classified information (e.g., store, use, transport, protect, and destroy)
- this module covers what you need to know to protect classified information at IN CONFIDENCE, SENSITIVE, and RESTRICTED classification levels.

Module 4: How to classify national security information (protectivesecurity.govt.nz)

Duration: 30 minutes

Audience: Government employees, contractors, and suppliers who hold a national security clearance and who create national security related information.

This module builds on knowledge you gained from all previous modules and looks specifically at how to classify information and assets relevant to New Zealand's national interest and national security.

On completion of this module you will understand:

- what are your obligations as a national security clearance holder
- what is national security information
- how to classify national security information
- how to apply national security markings to information or assets.

Module 5: How to protect national security information (protectivesecurity.govt.nz)

Duration: 15 minutes

Audience: Government employees, contractors, and suppliers who hold a national security clearance and who handle national security related information.

This module builds on knowledge you gained from all previous modules and looks specifically at how to protect information and assets relevant to New Zealand's national interest and national security.

On completion of this module you will understand:

- how access is controlled through the need-to-know principle, national security clearances, identity, and permissions
- how to securely handle national security information (e.g. store, use, transport, protect, and destroy).

See Identifying National Security Information for more information.

Security Classification System resources

Getting started

- Classification Handbook (protectivesecurity.govt.nz)
- Classification Quick Guides (protectivesecurity.govt.nz)

User Training Materials

- Module 1: Introduction to classification (ldc.govt.nz)
- Module 2: How to classify information (ldc.govt.nz)
- Module 3: How to protect information (ldc.govt.nz)
- Module 4: How to classify national security information (ldc.govt.nz)
- Module 5: How to protect national security information (ldc.govt.nz)

More resources

- Classify it! (protectivesecurity.govt.nz)
- Case studies (protectivesecurity.govt.nz)
- Frequently asked questions (protectivesecurity.govt.nz)

Glossary

680. See PSR Glossary (protectivesecurity.govt.nz) for more terms and definitions.

Term	Definition
Availability	Availability means that authorised users have access to the information that they need. See also Integrity and Confidentiality.
Classification System	New Zealand Government Information Security Classification System. This is New Zealand government's administrative system (principles, policies, guidance, tools, and resources) for the appropriate classification and handling of government information to ensure it is appropriately used, managed, and protected.
Classified information	Classified information is any government information that requires security and special handling to protect it. The information is generally protectively marked with the classification level (e.g. IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET) and may also include other endorsement or compartmented markings. See also Protective marking, Endorsement marking, and Compartmented marking.
Compartmented marking	A compartmented marking is an additional protective marking that is combined with the classification and endorsement marking (if applicable) indicating that the information is in a specific compartment. This word could be a codeword or 'Sensitive Compartmented Information (SCI)'. See also Protective marking, Need to know, Endorsement marking, and SCI.
Compromise	Information compromise is the intentional or unintentional unauthorised disclosure, removal, tampering, destruction, or misuse of the information.
Confidentiality	Confidentiality means that information is protected from unauthorised disclosure or access. See also Integrity and Availability.
Decision-useful information	Information is decision useful when it assists users to make good decisions or informs the development of advice to decision-makers. To be decision-useful, the information needs to be high-quality, timely, and accurate.
Declassification	Declassification is the process for reviewing the protective marking on information with the objective of removing or downgrading classifications to facilitate the public release of information.

Disposal	In the context of information and records, disposal means the decision-making processes for retaining, transferring or destroying information and records.
Endorsement marking	An endorsement marking is an additional protective marking that combined with the classification, warn people that information has special handling requirements. The endorsement marking may indicate the specific nature of information, temporary sensitivities, limitations on availability, or conditions for handling. See also Protective marking and compartmented marking.
Government information	Government information is all information, regardless of form or format, from documents through to data, 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, contractors, or consultants and includes public records, email, metadata, and datasets.
GPSL	The Government Protective Security Lead (GPSL) is a leadership role appointed by the Public Service Commissioner to the Director-General of the New Zealand Security Intelligence Service (NZSIS).
Integrity	Integrity means that information is protected from unauthorised changes to ensure it remains reliable and correct. See also Availability and Confidentiality.
National interest	National interest means the maintenance of New Zealand's good international reputation and bilateral relations, public confidence in the areas of tourism, trade, the economy and government, and the security and safety of all New Zealanders.
Need-to-know	A principle that a user must have a legitimate reason to access and use information or equipment to meet an operational need.
Need-to-share	A principle that government information needs to be appropriately shared to enable the protection of New Zealand and New Zealanders from threats, and to realise the potential of information to aid government effectiveness and enable wellbeing of New Zealanders.
Open information	Open information is unclassified information that has been made available to the public for their use and sharing. See also Unclassified information.
Paragraph marking	Paragraph marking is the practice of marking the classification level of a section of information within a document, email, or dataset. This informs the user of which sections contain the information of

	highest classification and enables more appropriate sharing of information.
Partner	Partner refers to any individuals, groups, organisations, or governments where information is shared.
Protective marking	Protective marking is the practice of marking the information with its classification, endorsement markings, and compartmented markings (if applicable) such as within paragraphs, emails, documents, metadata, or systems to inform readers and users of their obligations for securely handling and protecting the information.
PSR	Protective Security Requirements (PSR) outlines the Government's requirements for managing personnel, physical, and information security. The Classification System is a core foundation to the PSR. The PSR was approved by Cabinet in 2014 [CAB (14) 39/38]
Safe hand	A method of transporting an article in such a way that the article is in the care of an authorised officer or a succession of authorised officers who are responsible for its carriage and safekeeping. The purpose of sending an article using safe hand is to establish an audit trail that allows the sender to receive confirmation that the addressee received the information.
SCI	Sensitive Compartmented Information. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Intelligence Community. See also Compartmented marking, Need to know.
Security	The controls and measures that an organisation uses to protect their people, information and assets.
Stewardship	Stewardship is the careful and responsible management of something. In the context of this guide, it is the careful and responsible management of government information to benefit all New Zealanders.
Unclassified information	Unclassified information is government information that would have a low impact on individuals, organisations or New Zealand's national interest if it were compromised. It doesn't need special security or handling over and above the standard protections that apply to all government information and therefore does not require classification or protective marking to keep it secure.