# **Sample Template Only** **<<Organisation>> Classification Policy**

Contents

[Sample Template Only <<Organisation>> Classification Policy 1](#_Toc98150429)

[Introduction 2](#_Toc98150430)

[Purpose 2](#_Toc98150431)

[Scope 2](#_Toc98150432)

[Definitions 2](#_Toc98150433)

[Relevant Legislation 3](#_Toc98150434)

[Official Information Act 1982 (OIA) 3](#_Toc98150435)

[Local Government Official Information and Meetings Act 1987 (LGOIMA) 3](#_Toc98150436)

[Privacy Act 2020 (Privacy Act) 3](#_Toc98150437)

[Public Records Act 2005 (PRA) 4](#_Toc98150438)

[Inquiries Act 2013 (Inquiries Act) 4](#_Toc98150439)

[Policy Principles 4](#_Toc98150440)

[Responsibilities 5](#_Toc98150441)

[Policy 9](#_Toc98150442)

[<<ORGANISATION>> will ensure everyone understands and can fulfil their classification obligations 9](#_Toc98150443)

[<<ORGANISATION>> will classify government information appropriately 9](#_Toc98150444)

[<<ORGANISATION>> will handle government information securely 10](#_Toc98150445)

[<<ORGANISATION>> will share government information appropriately 11](#_Toc98150446)

[<<ORGANISATION>> will de-classify government information systematically 11](#_Toc98150447)

[<<ORGANISATION>> will measure and improve the performance of classification over time 11](#_Toc98150448)

[Related policy/ guidance 11](#_Toc98150449)

[Approvals 11](#_Toc98150450)

Words in black font are suggested policy content.

*Words in red italics highlight areas where agencies will need to contextualise the template with their own information.*

## Introduction

1. This policy outlines the statutory and business requirements and the framework for security classification of government information for <<ORGANISATION>>.

## Purpose

1. This policy outlines how <<ORGANISATION>> complies with the New Zealand Government Information Security Classification System (Classification System).
2. <<ORGANISATION>> fully supports the Classification System and its
	1. Principles of Organisational Accountability, Personal Responsibility, Information Sharing, and Declassification.
	2. Commitment to encourage and support partnership and collaboration as envisaged by Te Tiriti o Waitangi
	3. Objective to enable stewardship of government information for the benefit of all New Zealanders - He taonga te parongo, tukuna kia tina.
3. This policy aims to define how government information will be protectively marked and protected to maintain its confidentiality, integrity, and availability.

## Scope

1. This policy applies to all government information related to business activities performed on or on behalf of <<ORGANISATION>>.
2. Government information is all information, regardless of form or format, from documents through to data. This includes all written documents, whether paper or electronic; all records of spoken transactions including meetings, telephone calls, and all data held within <<ORGANISATION>> information systems. This includes information from or exchanged with the public, external partners, foreign governments, contractors, or consultants and includes public records, email, metadata, and datasets.
3. This policy should be read in conjunction with the following <<ORGANISATION>> policies:
	1. *Information Management Policy*
	2. *Information Security Policy*
	3. *Information Requests Policy*
	4. *Information Declassification Policy*
	5. *Other relevant policies and policy statements that apply*
4. All <<ORGANISATION>> policy, systems, and procedures pertaining to government information classification, use, handling, security, sharing, declassification, management, release, archive or disposal are to be consistent with this policy.
5. This policy applies to all employees, suppliers, contractors, and any persons who are involved in creating, managing, or handling government information of <<ORGANISATION>>.
6. This policy is approved by the <<Agency Head>> and should be reviewed three years from the date of signing or earlier as required.

## Definitions

1. **Classification System** 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.
2. **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.
3. **Unclassified information** is any government information that doesn’t need increased security and therefore does not require protective marking but still requires an appropriate degree of protection.
4. **Classified information** is any government information that requires increased security and special handling to protect it. The information is generally protectively marked.
5. **Protective marking** is the practice of marking the information with its classification, endorsements, and compartmented markings (if applicable) such as within paragraphs, emails, documents, metadata, systems, or made verbally to inform users of their obligations for securely handling and protecting the information.
6. **Protection** refers to the security measures and handling requirements put in place to protect the information’s availability, integrity, and confidentiality.
7. **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]
8. **New Zealand Information Security Manual** (NZISM) is the Government’s manual on information assurance and information system security.

## Relevant Legislation

### Official Information Act 1982 (OIA)

1. The OIA aims to increase the availability of official information to New Zealanders. It provides the legislative basis for the release of official information. Official information is a subset of all government information. The Classification System sits alongside the OIA as an added protective measure with specific emphasis on how certain government information should be handled.
2. Sections 6, 7, and 9 of the Act describe justifiable reasons and harm conditions that may exempt or conditionally exempt the information from release. These sections provide the foundational harm tests under the Classification System risk assessment process.
3. The justification for withholding any particular information must outweigh the justification of the public interest of its disclosure.

### Local Government Official Information and Meetings Act 1987 (LGOIMA)

1. The LGOMA aims to increase the availability of official information held by local authorities to New Zealanders.
2. Sections 6 and 7 of the Act describe justifiable reasons and harm conditions that may exempt or conditionally exempt the information from release. These sections should also form foundational harm tests under the Classification risk assessment process for official information held by local authorities.

### Privacy Act 2020 (Privacy Act)

1. The Privacy Act promotes and protects individual privacy by setting out the principles for how public sector agencies should collect, use, hold, disclose and allow access to personal information.
2. Information privacy principle 11, principle 12, sections 49 to 53 of the Act set out the limits on disclosure of personal information and the justifiable reasons and harm conditions that may prevent disclosure of personal information.
3. Part 7 of the Act sets out the conditions that enable information sharing in accordance with an approved information sharing agreement to facilitate the provision of public services or to facilitate law enforcement.
4. Part 8 of the Act set out the reasons why transferring personal information may be prohibited including compliance with overseas requirements such as UK’s requirements for GDPR or OECD guidelines.

### Public Records Act 2005 (PRA)

1. The PRA supports the accountability of Government (and its agencies) by ensuring that full and accurate records are created and maintained, by providing for the preservation of, and public access to, records of long-term value.
2. Part 3 (Public Access) of the Act sets out the requirement to classify the access status of public records as either open or restricted and defines the basis and rules for determining the access status

### Inquiries Act 2013 (Inquiries Act)

1. The Inquiries Act provides for the establishment of both public and government inquiries to inquire into matters of public importance and sets out the powers, duties, and privileges of inquiries and procedures for inquires including in relation to obtaining or disclosing of information.
2. Sections 19 to 27 of the Act set out the duties, powers, immunities, and privileges related to the receiving and disclosure of information as evidence.
3. Section 32 and 33 of the Act sets out how inquiries apply the OIA and PRA to the official information that they collect as part of inquiry.

## Policy Principles

1. The <<ORGANISATION>> will adhere to the following policy principles to support the adoption of the Classification System and enable our people to fulfil their obligations to classify, declassify, share, and handle information correctly and safely.

**Policy principle 1:** Classification aims to meet government and community expectations that the organization will be transparent and accountable for its activities while maintaining justifiable protections in accordance with the requirements of the Public Records Act, the Official Information Act 1982, the Privacy Act 2020, other relevant legislation, or contained in relevant international arrangements or agreements.

**Policy principle 2:** Government information will be considered open, unless there is a compelling reason to withhold it as defined within this policy.

**Policy principle 3:** Classification and declassification decisions rest with the originator and the organisation or government that controls the information. As the owner of information, we will ensure that classifications and protective markings are reviewed at agreed points in the information lifecycle (e.g. during drafting, at release, when updated, upon request for release, and at agreed review points as defined within this policy for the information types).

**Policy principle 4**: Everyone who works in or with the public sector must take responsibility to understand and fulfil their obligations to classify, declassify, and handle information correctly in line with this policy and legislative, regulatory, and other organisational obligations.

**Policy principle 5:** Classification and declassification decisionsare based on the best information available and are based on a risk assessment that considers the level of harm and the likelihood of compromise of the information.

**Policy principle 6**: Classification drives the appropriate security measures (personnel, physical, and information security) of the information to ensure its availability, integrity, and confidentiality commensurate with its classification and protective markings.

**Policy principle 7:** Some classified information held by the organization originates from other governments, agencies, third parties, or individuals and there are limits on our ability to declassify, share, or release it without the agreement of the originator or controlling government or organisation or conditions set out in the relevant legislation. However, the absence of permission from another party to release information does not absolve the organisations from its obligations under New Zealand legislation.

## Responsibilities

1. This section highlights the roles and responsibilities for oversight and functional responsibilities for classification.

|  |  |
| --- | --- |
| Role | All employees, contractors, suppliers, or persons using government information |
| Function | Everyone who works in or with <<ORGANIZATION>>, including employees, contractors, and suppliers, has a duty to classify, declassify and handle information appropriately. |
| Responsibilities | * **Duty to safeguard** – Individuals are responsible for protecting government information and assets in their care in line with the classification and protective marking. Accidentally or deliberately compromising government information without authorisation may lead to harm or damage and can be a criminal offence under relevant legislation (e.g. Crimes Act 1961, Criminal Disclosure Act 2008, Summary Offences Act 1981.)
* **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 likelihood of compromise.
* **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.
* **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.
* **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.
* **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.
* **Don’t withhold information inappropriately** – Individuals must not use classification to withhold information inappropriately. For example, government information should not be withheld to:
	+ hide violations of law, inefficiency, or administrative error
	+ prevent embarrassment to an individual, organisation, agency, or the government
	+ restrain competition
	+ prevent or delay the release of information that does not need protection in the public interest.
 |

|  |  |
| --- | --- |
| Role | Agency Head / Chief Executive  |
| Function | 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. |
| Responsibilities | * Agency head will 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.
* Agency head will champion, lead, oversee, and delegate responsibility for classification functions and responsibilities as appropriate to:
	+ Establish an organisational classification policy and procedures in line with the Classification System and relevant legislation and ensure that all people who handle government information do so correctly and safely.
	+ 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.
	+ Build an effective information management culture that:
		- understands the harm of over-classification and under-classification
		- applies appropriate measures to protect government information commensurate with its protective marking
		- values secure and effective information sharing with partners and openness and transparency with the public
		- encourages a no blame culture that focuses on learning and improving classification and appropriate handling decisions.
	+ In line with PSR GOV8 (Assess your capability), assess the organisation’s classification capability and performance using the PSR Capability Maturity Model and annual PSR assurance process as part of their overall protective security programme.
 |

|  |  |
| --- | --- |
| Role | Classification owner (e.g. Information Manager or Information Security Manager) |
| Function | Classification owner is responsible for the effectiveness of classification policy and practice within <<ORGANISATION>>  |
| Responsibilities | * Classification owner ensures that the classification policy and practice remain fit for purpose for <<ORGANISATION>>.
* The Classification owner is responsible for:
	+ Working across the organisation to develop and implement a fit-for-purpose classification policy and set of procedures that achieves the desired outcomes.
	+ Assesses the classification capability of the organisation to establish the baseline maturity and develop and agree a plan for improvement.
	+ Solicits, builds, and maintains an informal community of Classification champions across the organisation who will help people to make good classification and secure handling decisions
	+ Working with learning and development and other subject matter experts to build, maintain and roll out appropriate classification and security education and training materials that deliver on classification learning needs for <<ORGANISATION>>.
	+ Creates and launches communication campaigns that emphasise desired behaviours and information management culture:
		- understands the harm of over-classification and under-classification
		- applies appropriate measures to protect government information commensurate with its protective marking
		- values secure and effective information sharing with partners and openness and transparency with the public
		- encourages a no blame culture that focuses on learning and improving classification and appropriate handling decisions.
	+ Establishes, monitors, and reports on the success of the classification policy and programme.
	+ As part of the annual PSR assurance process, leads the assessment of the organisation’s classification capability and performance using the PSR Capability Maturity Model and reporting.
 |

|  |  |
| --- | --- |
| Role | Classification champion (optional role if needed) |
| Function | Classification champions support individuals to make good classification, declassification, and handling decisions.  |
| Responsibilities | * Classification champion is a subject matter expert on how the classification policy is applied within a specific unit or function of <<ORGANISATION>> .
* Classification champion will support individuals in their business unit or function to apply the classification policy consistently and accurately:
	+ Understand the classification policy and translate that into specific procedures and criteria within their specific unit’s context.
	+ Help people to make good classification and secure handling decisions.
	+ Identify people who would benefit from additional classification or other information management training. This may include training on how to securely handle government information, including how to classify it, how to share it, and how to declassify it.
	+ Exemplify the desired behaviours and information management culture:
		- understands the harm of over-classification and under-classification
		- applies appropriate measures to protect government information commensurate with its protective marking
		- values secure and effective information sharing with partners and openness and transparency with the public
		- encourages a no blame culture that focuses on learning and improving classification and appropriate handling decisions.
	+ Leads occasional audits of classification and declassification decisions to assess how well the team are consistently and accurately assessing the risk and harm and using these are learning opportunities as inputs to improve policy, procedures, training, and practice.
	+ Report to the Classification owner with ideas for improvement to ensure the policy and practice remain fit-for-purpose.
 |

|  |  |
| --- | --- |
| Role | Partner information liaison (optional role if needed) |
| Function | Partner information liaison owns the relationship with specific partner governments, agencies, third parties, or groups and is the subject matter expert into the core obligations and processes for appropriately handling and managing partner information.  |
| Responsibilities | * Partner information liaison is a subject matter expert on how the classification policy is applied to partner information within the context of specific partner agreements (whether formed by legislation, formal information sharing agreement, or informal cooperation).
* Partner information liaison will support individuals in to correctly handle and manage partner information:
	+ Establish specific partner information handling procedures in line with the classification policy.
	+ Help people to make good de-classification and secure handling decisions in line with partner information agreements
	+ Liaise with the partner on requests for partner information release to agree the risk assessment and harm of release and obtain permission for release as appropriate.
	+ Exemplify the desired behaviours and information management culture:
		- understands the harm of over-classification and under-classification
		- applies appropriate measures to protect government information commensurate with its protective marking
		- values secure and effective information sharing with partners and openness and transparency with the public
		- encourages a no blame culture that focuses on learning and improving classification and appropriate handling decisions.
	+ Leads occasional audits of partner information to assess how well the team are consistently and accurately applying partner information handling requirements and using outcomes as learning opportunities and inputs to improve policy, procedures, training, and practice.
	+ Report to the Classification owner with ideas for improvement to ensure the policy and practice remain fit-for-purpose and aligned to our obligations for partner information management.
 |

## Policy

### <<ORGANISATION>> will ensure everyone understands and can fulfil their classification obligations

1. <<ORGANISATION>> will provide their people (all employees, suppliers, contractors, and any persons who are involved in creating, managing, or handling government information of <<ORGANISATION>>) with timely and ongoing classification training and guidance. This training forms part of the mandatory information management and security curriculum.
2. All people will take responsibility to participate in classification training and ensure that they understand and fulfil their obligations to classify, share, declassify, and handle information correctly and securely. Each person will be assessed on their understanding and performance.

### <<ORGANISATION>> will classify government information appropriately

1. <<ORGANISATION>> creates and collects government information where it is necessary and relevant to perform its function. Classification decisions on government information will be subject to an information compromise risk assessment and harm test and will be protectively marked in accordance with this policy’s principles and the *<<ORGANISATION>>* *security classification guidelines*.
2. Not all information created or collected by <<ORGANISATION>> requires classification. This information is called unclassified information and *will / may / will not /* be protectively marked with UNCLASSIFIED.
3. <<ORGANISATION>> receives information from a variety of sources; including domestic and foreign partners, agencies within the public and private sector, as well as individuals. Sourced information must be classified at a level not less than that in force by the partner or organisation and in accordance with *<<ORGANISATION>>* *partner information guidelines*.
4. Classifications and other protective markings will be reviewed over the information’s lifecycle to ensure that protective markings remain appropriate based on the harm of its compromise. For example, the information will be reviewed at these points:
	1. Drafting
	2. Publishing
	3. Disseminating
	4. Editing / changing
	5. Archiving / deleting
	6. Request for clarification or justification
	7. Request for information release
	8. Review date expiry
	9. Random information audits
	10. Declassification (see separate Declassification policy and criteria.)

### <<ORGANISATION>> will handle government information securely

1. Classification drives the appropriate security of the government information and must be protected to ensure its availability, integrity, and confidentiality. <<ORGANISATION>> applies protections to government information in compliance with the relevant legislation, Protective Security Requirements (PSR), New Zealand Government Information Security Classification System (Classification System), New Zealand Information Security Manual (NZISM), and in accordance with *<<ORGANISATION>>* *security classification guidelines* and *<<ORGANISATION>>* *partner information guidelines.*

#### Controlling access to government information

1. *This section should reference any related handling instructions, organisational policy and guidance relating to how personnel security, need-to-know, need-to-share, and access controls apply to government information.*

#### Storing and filing government information

1. *This section should reference any related handling instructions, organisational policy and guidance relating to the storage and filing of government information.*

#### Using, copying, and reproducing government information

1. *This section should reference any related handling instructions, organisational policy and guidance relating to the usage, copying, and reproducing of government information.*

#### Removing, transmitting, and transporting government information

1. *This section should reference any related handling instructions, organisational policy and guidance relating to the removal, transmission, or transport of government information.*

#### Archiving or disposing government information

1. *This section should reference any related handling instructions, organisational policy and guidance relating to the archiving and disposal of government information.*

### <<ORGANISATION>> will share government information appropriately

1. *This section should reference any sharing agreements in place with external parties, organisational policy and guidance relating to the sharing of government information including links to registers for those who hold partner information liaison roles.*
2. *This section should detail the how partner information security and management requirements will be managed, adhered to and monitored.*
3. *This section should also define how originator control will be maintained over the information’s lifecycle when information is shared with external parties and how communication of changes to the classification and protective markings will be accomplished.*

### <<ORGANISATION>> will de-classify government information systematically

1. *This section should reference the organisational policy and guidance relating to the declassification of government information including proactive release, responding to requests for release, and archival declassification and release.*

### <<ORGANISATION>> will measure and improve the performance of classification over time

1. *This section should reference the organisational policy and guidance relating to the mechanisms put in place to measure the performance of the classification system.*

## Related policy/ guidance

1. Related policy and guidance documents include:
	1. <<ORGANISATION>> security classification guidelines
	2. <<ORGANISATION>> partner information guidelines
	3. Government Information Security Classification System Policy
	4. PSR Classification Guidance and Website content
2. *This paragraph should reference any related organisational policy and guidance, i.e. those that individuals involved in declassification need to be specifically aware of.*

## Approvals

1. *This section should include a dated signature block confirming approval and ownership of the policy, similar to the table below.*

|  |  |
| --- | --- |
| Approved by: | Chief Executive*Signature* |
| Approval Date: |  |
| Policy Owner: |  |
| Contact Details: |  |
| Review Date: |  |