New Zealand Government Information Security Classification System Policy 2022

The Classification System is mandated for use by the Protective Security Requirements Information Security requirement:

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.

To meet this mandatory requirement, your agency must implement the 2022 Classification System policy and requirements detailed in the next section.

2022 policy and requirements

Policy overview

The Government Information Security Classification System (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 this policy on 23 March 2022.

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.

The Classification System is mandatory for use within government departments, ministerial offices, the NZ Police, and the NZ Defence Force. 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].

The 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 Classification System.

This Government Information 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

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

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.

The Classification System policy is based on these principles.

- Organisational accountability
- Personal responsibility
- Information-sharing
- Information declassification

Principle 1: Organisational Accountability

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

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

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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

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

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.

The following requirements should be considered when taking personal responsibility for classifying, declassifying, and handling government information.

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.)

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.

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 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. Agencies should encourage a no blame culture that focuses on learning and improving classification and handling decisions over time.

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.

Principle 3: Information-sharing

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

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.

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

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.

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.

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.

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.

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

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

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.

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

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 – 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.

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.

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.

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.

For more information, visit **https://protectivesecurity.govt.nz/classification-system**