MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

24 June 2026

Tēnā koe

Official Information Act Request

Thank you for your email of 8 and 16 June 2026 to the Ministry of Social Development (the Ministry), requesting information about the Review of Decision (ROD) process and the Ministry's records management process.

I have considered your request under the Official Information Act 1982 (the Act). Please find my decision on each of your requests set out separately below.

- **ROD Process – 8 June 2026**

A ROD application is an opportunity for Ministry clients to challenge the Ministry regarding decisions that clients do not agree with, pursuant to section 391 of the Social Security Act 2018 (the SSA). The process starts with an administrative review generally referred to as an internal review and can progress through to a Benefits Review Committee (BRC) hearing. The ROD process can be ended before a determination is made by a client voluntarily withdrawing their ROD application. Attached as **Appendix One** is the Ministry's ROD Process summary.

The Ministry also has some publicly available information about the process here:

- www.workandincome.govt.nz/about-work-and-income/feedback-and-complaints/review-of-decisions.html
- www.msd.govt.nz/about-msd-and-our-work/contact-us/review-of-decision/review-of-decision-flow-chart-long-description.html

Additionally, the below links to previous Official Information Act responses may contain information that you will find useful:

- 09052023-information-on-review-of-decision-applications-and-benefit-review-committees-statistics-from-the-annual-report.pdf
- 30062023-request-for-all-information-about-the-complaints-process-for-current-clients-including-policy-and-statistics-over-the-last-five-years.pdf

Depending on the benefit being reviewed, there is information about the Review of Decision on our operational policy guidelines website here: www.workandincome.govt.nz/map/.

- **Information Management Policy – 16 June 2026**

I have attached five documents marked as **Appendices Two to Six**. These are:

2- *Ministry of Social Development Information Governance Policy*
3- *Minimum Metadata Capture standard*
4- *Information Retention and Disposal Standard*
5- *Information Migration Standard*
6- *Information Classification Standard*

These are released to you in full. You can also find more information about this on our website at: www.msd.govt.nz/about-msd-and-our-work/publications-resources/planning-strategy/information-data-and-analytics-strategy-2022/data-analytics-information-roadmap-initiatives.html.

I will be publishing this decision letter, with your personal details deleted, on the Ministry's website in due course.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with my decision on your request, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Ngā mihi nui

pp.
Anna Graham
General Manager
Ministerial and Executive Services

The Review of Decision Process Summary

In keeping with the provisions of legislation and Ministry policy, any application to the Ministry for a review of decision, triggers the start of a review process. Our Team is involved with the inital stages of the judicial review process starting with an Internal Review and culminating with a decision being taken by a Benefits Review Committee.

On this Page:

The Internal Review stage

The first part of the review process comprises an 'Internal Review' by the site that made the decision under review. The Service Centre Manager of the site in question examines the decision under review in the light of legislation and Ministry policy. This part of the process is primarily an administrative process and is not a legal requirement. It is implemented in order to weed out incorrect decisions and to correct them before they are escalated to the next stage. If the site in question upholds the initial decision the review application moves on to the next stage.

The Report to the BRC stage

At this stage the original decision under review is re-examined, any new information provided by the Applicant is taken into account and a comprehensive Report to the Benefits Review Committee, covering the perspectives of both the Applicant and the Ministry is written up. The Benefits Review Committee (BRC) is a review body that is established to make correct and fair decisions with regard to procedure and law. A copy of the Report to the BRC is sent to the Applicant and each panel member of the Benefits Review Committee. A suitable date for 'Hearing' the case by the Benefits Review Committee is scheduled and the Applicant is advised.

The BRC Hearing

The composition of the Benefits Review Committee is in accordance with Schedule 7 of the Social Security Act 2018. It comprises three panel members. Two of the panel members are employees of the Ministry, who have had no involvement with the original decision. The third panel member is an independent person of high standing in nthe community appointed by the Minister. This ensures impartiality, transparency and fairness in the decision making process.

Benefits Review hearings are a chance for a review panel to take a fresh look at decisions made by the Ministry of Social Development.

On the scheduled hearing date, the Benefits Review Committee convenes with the Applicant and a representative of the Ministry. The panel hears presentations from both the Ministry and the Applicant. However, if the Applicant fails to put in an appearance the panel considers only the facts of the case presented in the report provided to it and in this case the Ministry will not attend the hearing either. The Committee re-examines the decision under review and considers the perspectives of both the Applicant and the Ministry giving due regard to any natural advantage that the Ministry may have in the situation.

The Report of the BRC

After the hearing the Benefits Review Committee deliberates on the issue under review in the light of legislation. It tries to arrive at a decision which is both fair to the Applicant and at the same time, within the bounds of what the Ministry can do under legislation.

The decision of the Committee is conveyed to the Applicant and the Ministry through a letter enclosing a copy of the decision report written by the Chairperson of the Committee. Applicants are advised of the Social Security Appeals process where they could seek further redressal if they are not satisfied with the decision of the Benefits Review Committee.

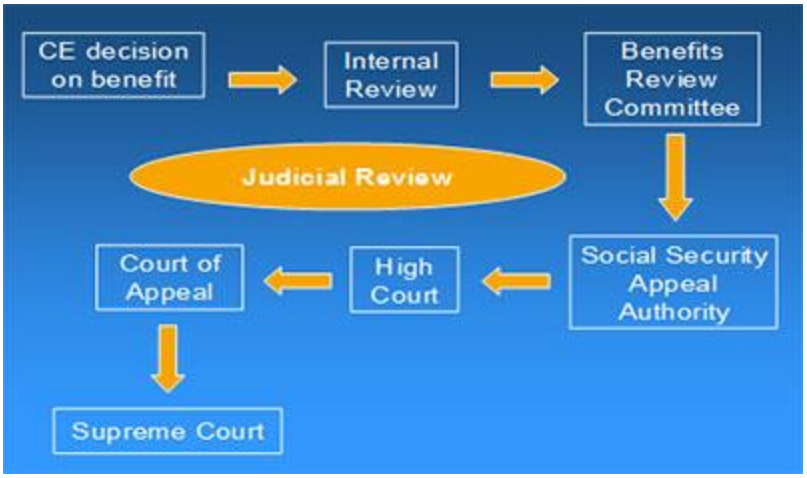
The Out of Time Review process

An Out of Time review is where a Review of Decision is lodged outside of the three month timeframe provided for in section 392 of the Social Security Act 2018.

When a review is lodged Out of Time a slightly different process needs to be followed. This includes a hearing being held by the Benefits Review Committee to determine whether or not the review will be heard. Please refer to the link below for all you need to know about the Out of Time process.

Out of Time reviews [http://doogle/resources/helping-staff/procedures-manuals/review-decisions/out-of-time.html]

The Judicial Review Process



The flow chart on the left, shows the entire judicial review process available to any client wishing to review any decision of the Ministry.

The Ministry is involved with the first, second and third stages of the process known as the Benefits Review Committee process. This includes the conduct of an Internal Review, the writing of a report to the Benefits Review Committee, organising a review Hearing by the Committee and the writing of a decision report by the Committee. The Benefits Review Committee process is an important part of ensuring that correct decisions are made by the Ministry on a case by case basis.

Content owner: Review of Decision **Last updated:** 21 December 2020

Information Governance Policy

Last Review Date:	November 2024
Next Review Date:	November 2026
Approved by:	Organisational Health Committee
Owner:	General Manager Information (CISO, CPO)

Purpose

This policy defines the principles, roles, and responsibilities which support the Ministry of Social Development (the Ministry) in upholding its Information Governance responsibilities to the New Zealand Government and public. The principles found in this policy set the governing direction and intent for Information Governance. Underpinning this policy are standards, patterns, processes, and guidance material which collectively operationalise the principles in this policy and align the Ministry's Information culture and decision-making.

Policy Statement

The Ministry holds and uses information (including personal information and data) about people that impacts their lives. Information is taonga, and as its stewards we must both use it responsibly and protect it while it is in our care.

Effective information governance requires the Ministry to understand the information it holds, define who is responsible for that information, and know how that information is being used. Additionally, it requires the Ministry to have assurance that its information is protected, is managed appropriately, and its staff are acting responsibly when using information.

Scope

This policy applies to all Ministry staff including contractors; all information and data held and used by the Ministry; and all activity conducted by third parties on behalf of the Ministry.

Policy Principles

The following principles must be understood and followed to ensure alignment with the purpose of this policy.

1. The Ministry's information assets are identified and appropriately protected based on legislative requirements, information value and risk culture

The Ministry manages information assets in accordance with the requirements defined in key legislation such as the Public Records Act 2005, Privacy Act 2020, and the Official Information Act (1982), along with policy guidance such as the Protective Security Requirements (PSR). The Ministry's standards and other guardrails define the measures which set the baseline for how information assets are collected, secured, stored, used, and managed using a risk-based approach.

2. All information assets held by the Ministry have responsible Information Asset Owners to ensure they are managed and used appropriately

An information asset has value to the Ministry from the point of creation or collection through to its eventual disposal. Information Asset Owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are understood, managed and monitored throughout the information asset's lifecycle. Information Asset Owners are also responsible for how their information assets are used, including use with algorithms or other tools. Any legal and regulatory requirements applicable to the collection, storage, use, disclosure or disposal of the information must be understood by the Information Asset Owner.

3. Information assets are fit-for-purpose to promote informed decision-making

Consistently and continuously maintaining the quality and integrity of Ministry information assets ensures people use authoritative information. The information collected, used, and shared by the Ministry is appropriate for the purposes it is intended and collected for, and contributes towards better insights, better decisions, and better lives.

4. The Ministry partners with tangata whenua in decision-making about information held by the Ministry to support Māori

The Ministry fosters collaborative relationships with Māori communities to ensure their voices are heard and respected in decisions about information held by the Ministry that impacts their lives. The Ministry values the trust placed in it by Māori and is dedicated to embedding Māori perspectives into the way it cares for and manages Māori information. Upholding its responsibilities to its Accord partners, the Ministry is committed to working alongside key partners to support decisions about how Māori information is governed.

5. The protection and responsible use of Ministry information is everyone's responsibility

Ministry staff are responsible for handling information appropriately while it is in our care. Ministry technology and processes play a key role in providing a layer of protection over information, and our awareness of information risk and its acceptable use is just as important. The Ministry expects staff to act in a timely and coordinated manner to prevent or respond to breaches of, and threats to, information.

Roles and Responsibilities

Everyone that works for or is contracted to the Ministry has a responsibility to comply with this policy. The responsibility of each role specifically relevant to this policy is set out in the table below:

Person/Party	Responsibility
All Staff	All staff are responsible for: • Complying with the Ministry's information policies • Following information guidance and training • Identifying and reporting information security, information management, and privacy incidents • Escalating risks, as needed, to their manager
Managers	All managers are responsible for: • Leading and facilitating regular information discussions with their teams • Ensuring their teams are familiar with the Ministry's information policies and guidance; use approved tools, and comply with the Ministry's information governance approach • Providing direction on acceptable behaviours to their teams • Modelling good information practice through their actions and behaviour • Identifying and escalating information risks, as appropriate, to ensure information is managed effectively at the appropriate level and in a timely way • Reporting any information security or privacy incidents to their line manager

Person/Party	Responsibility
Information Asset Owners	All information assets owners are responsible for: • Leading and championing a culture that values protection and responsible use of information; • Understanding which information assets, they are accountable for, their value, where they come from, and how they are used; • Knowing who has access to that information and why and ensuring that access is controlled and reviewed continuously; • Ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored; and • Ensuring their information assets are fully utilised in line with responsible information use. The information asset owner must understand the value of each information asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information asset. At the Ministry, Information Asset Owners will typically be assigned at the Tier 3 senior leader level, reporting directly to Deputy Chief Executives (DCEs).
Information Stewards	Information Stewards are responsible for: • Maintaining specialist knowledge about the information in their business area. • Ensuring information is available for its intended purpose; • Managing and maintaining information assets based on MSD standards, policies, and other guardrails, including data quality, integrity, and metadata; • Maintaining and updating an inventory of information assets; • Monitoring and optimising the lifecycle of information to effectively manage risk and opportunities; • Collaborating with stakeholders across the business (System Owners, other Information Stewards, Business

Person/Party	Responsibility
	Capability owners, and Line 2 assurance functions, etc.) to implement the necessary guardrails; • The responsible use of information assets, enabling the organisation and other agencies where appropriate to gain maximum value from the information; and • Supporting information asset owners to make informed decisions about the management and use of their asset for the duration of its lifecycle. The Information Steward must keep the Information Asset Owner informed and aware of any risks or concerns surrounding the integrity or safety of the information. At the Ministry, Information Stewards will be assigned by the Information Asset Owners and are typically senior subject matter experts in their respective business areas.
Information Governance Committees	Information governance committees are responsible for overseeing and tracking the achievement of the Ministry's strategic objectives relating to information governance. They set the overall risk culture for the Ministry, which guides the way it responds to information risk and opportunity. These governance bodies must have membership from the Ministry's Leadership Team, as well as appropriate Māori representation, and have oversight of: • Information and IT security policies and strategies • Information standards and architecture • Obligations contained in the Protective Security Requirements (PSR), the Privacy Maturity Assessment Framework (PMAF), and the Archives New Zealand Information and Records Management Standard • Ministry decisions about ensuring there are adequate systems, processes, and controls in place to identify and manage information risk. At the Ministry, the Information Governance Committees consist of the Leadership team (LT), Organisational Health Committee (OHC), the Information and Protective Oversight Committee (IPSOC), the Transformation and Investment Committee, and Tai Nuku Design Committee.
Executive Sponsor Information	The Executive Sponsor champions the importance of information management among the organisation's leadership. The aim is for everyone in the organisation to see information management as an integral part of a business operating

Person/Party	Responsibility
	effectively. The Executive Sponsor Information is responsible for: • Ensuring that the strategy and policy adopted by the organisation supports information management • Being involved in strategic and operational planning to align information management with the corporate objectives and business activities of the organisation • Liaising with business units to ensure that information is integrated into work processes, systems, and services • Overseeing the budget for information and ensuring the resources needed to support information are known and sought in funding decisions • Ensuring that staff with appropriate skills to implement information strategies are employed, and regular upskilling is available • Monitoring and reviewing information to ensure that it is implemented, transparent and meets business needs The CE has delegated the Executive Sponsor Information role to the DCE Organisational Assurance and Communication (OAC).
Chief Security Officer	The Chief Security Officer (CSO) is responsible for having oversight of the Ministry's protective security practices in line with Protective Security Requirements (PSR). At the Ministry, the CSO is the DCE OAC.
Chief Information Security Officer	The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency. The CISO is responsible for cyber security requirements, and accountable for representing cyber security, leading a programme of cyber security continuous improvement, and managing a virtual team through a distributed security function. At the Ministry, the CISO is the General Manager (GM) Information. The GM Information is responsible for implementing and having assurance over this policy.

Person/Party	Responsibility
Chief Privacy Officer	The Chief Privacy Officer (CPO) sets the strategic direction for Privacy within their agency. The CPO is responsible for: • Dealing with any complaints from the Ministry staff or clients about possible privacy breaches • Dealing with requests for access to personal information, or correction of personal information • Acts as the liaison for the Ministry with the Office of the Privacy Commissioner • Advising the Ministry on the potential privacy impacts of changes to the organisation's business practices • Overseeing the function governing what the Ministry can and cannot do with personal information. At the Ministry, the CPO is the GM Information.
Information, Security and Identity Group	The Information, Security and Identity Group is responsible for: • Supporting MSD's strategic future – providing thought leadership on information security, privacy and information management across, as well as influencing information maturity growth across MSD and all of government • Delivering assurance - providing support to MSD in meeting its compliance responsibilities through an assurance programme to manage defined information risks. • Providing expert advice - providing specialist skills to ensure business processes and systems design align to good practice, including responsible use and protection of information assets and comply with information legislation and related regulations. • Delivering a foundational capability - providing direction, guidance tools, training and support for information capability improvements.
Strategy & Insights	The Strategy & Insights Group is responsible for: • Maintaining enterprise data resources, such as an enterprise data catalogue, enterprise data model, and their implementation into MSD's data warehouse, ensuring we can understand and

Person/Party	Responsibility
	access our authoritative data sets with confidence in their quality, timeliness, and consistency. • Driving MSD's approach to data and analytic products which support decision making, and ensuring we are recognising the potential value of a given use of data in trading off against risk. • Setting requirements for new data collection and standards around that data's quality and structure in order to be useful for analytics. • Supporting the Ministry to use and manage Ministry data, analytics, and evidence • Client and Business Intelligence and data science • Research and Evaluation to analyse data and produce insights that inform decision-making and provide evidence on what interventions work for whom • Data Management and data reporting.
Improvement, Systems and Technology (IST)	IST is responsible for enabling people and partners with improved services and effective technology so New Zealanders can easily access the support they need. IST, as system owners, are responsible for the overall operation of the system, including any outsourced services, telecommunications, and cloud. IST is part of the Transformation Group and are made up of service improvement and technology experts, including Technology Security and Identity
Ethics Advisor	The Ethics Advisor is responsible for: • Formulating, reviewing, and disseminating ethics-related documents, and providing guidance related to all ethical issues, including those relating to information (code of conduct, conflicts of interest, outside activities, etc.) At MSD, the Ethics Advisor is an independent ethics advisor commissioned by the GM Information.

Definitions

Word/ phrase	Definition
Algorithm	Algorithms are sets of instructions that enable computers to solve problems or complete tasks. There are many different types of algorithms for different purposes and outcomes. Algorithms can be simple or complex. All forms of 'AI' are complex algorithms.
Archiving	The process of preserving information that needs to be held over the medium or long term with low frequency of access, so that it retains its integrity and remains available for use by MSD and others until it is able to be disposed.
Information	Recorded information (including both personal information and data) in any form created or received and maintained as evidence of Ministry business. It includes, but is not limited to, documents, email correspondence, datasets, audit logs, metadata (including reaction emoji 😸), text messages, voice recording, social media, and web pages.
Information Asset	An Information Asset is an identifiable collection of information and data recognised as having value to the agency. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Lifecycle	The stages through which information passes, such as creation or collection, storage, access and sharing, use, maintenance and archiving, and disposal through destruction or transfer.
Information Governance	Enterprise Information Governance is a structured, consistent, and deliberate approach to managing, protecting, and using our information to support the Ministry's strategic objectives and fulfil mandated obligations. It unifies existing governance structures, clarifies decision-making processes, and identifies gaps across information-related capabilities. By embedding Te Ao Māori values and integrating the Information Accountability Framework and Information Policy Framework, it drives effective and accountable information management practices
Information Use	Information Use means everything that is done with information. This means not just active use, but also all parts of the information lifecycle (including collection and disposal). For the avoidance of doubt, information is being used when it is held in a database, even when that database is not actively being accessed.

Information Management	The process by which the Ministry ensures that information is managed across its lifecycle, such that it is accurate, relevant, and accessible; and that it is retained and disposed of appropriately in line with its value and its risk profile.
Information Security	Information Security relates to the protection of information regardless of its form (electronic or physical). The accepted definition of information security within government is: "measures relating to the confidentiality, availability and integrity of information".
Personal Information	Personal Information is defined under the Privacy Act 2020 as "Information about an identifiable individual…". It includes anything that relates to an identified person to be identified directly or indirectly, such as, but not limited to name, address, contact details, date of birth, signature, photographic image, Social Welfare Number, information about someone's health, sex life or orientation, their finances, religious, political or philosophical beliefs, race, biometric or genetic data.
Privacy	Privacy relates to the rights an individual has to control their personal information and how it's used. There is an obvious overlap between information security and privacy. This policy recognises the interdependence of one to the other.
Risk culture	The level of risk that an organisation is prepared to accept in pursuit of its objectives.

Minimum Metadata Capture Standard

Approved by:	General Manager Information Group, Hannah Morgan on 09/07/2024
Standard Owner:	General Manager Information Group
Next Review Date:	July 2026
Review Committee	Information Policies and Standards Working Group

1 Purpose

This standard describes the Ministry of Social Development (the Ministry) minimum expectations and requirements for capturing and managing metadata. Metadata helps organisations create reliable and trustworthy evidence of their business activities. It can be used to verify the authenticity and integrity of records, enable discovery and retrieval of information, and manage security and privacy requirements of information. Metadata comes in multiple forms – free-text, controlled lists and automatically generated.

This standard outlines the Ministry's obligations to capture and manage metadata under Archives New Zealand's Information and Records Management Standard, which supports organisations to meet their obligations under the Public Records Act 2005. The Information Governance Policy outlines how the Ministry manages information assets in accordance with legislative requirements, taking a risk-based approach, and ensures the integrity of Ministry information.

2 Scope

This standard applies to all information created, stored, and collected by or on behalf of the Ministry, which is subject to the Public Records Act 2005, except where that information is covered by Archives New Zealand's 'General Disposal Authority (GDA) 7 Facilitative, transitory, and/or short term value records' and the Information Group advises that its exclusion is appropriate.

Definitions can be found at the bottom of this standard.

3 Standard

3.1 Minimum Metadata Requirements

3.1.1 Metadata ***must*** be captured for all information assets stored in MSD approved repositories, so they can be appropriately managed throughout the information lifecycle.

3.1.2 Metadata forms part of the information asset so ***must*** be attached throughout the information lifecycle.

3.1.3 Metadata ***must*** be a design component of all approved repositories of Ministry information.

3.1.4 The System Owner ***must*** seek Information Group approval on what level metadata ***must*** be applied (e.g., to individual records, or whole datasets).

3.1.5 Audit and disposal metadata ***must*** be read-only. Other metadata ***must*** be read-only if advised by the Information Group.

3.1.6 To manage information assets through their lifecycle, the following metadata ***must*** be required. The Information Group will approve how they are applied.

Minimum metadata to assign when creating and managing information:

a) Unique identifier e.g., Object ID
b) Name / Title
c) Date created (or collected)
d) Business activity documented (which might be adequately described by the Disposal Class)
e) Information classification (in line with the classifications in scope of the MSD Information Classification Standard)
f) Creator e.g., individual and/or entity or system
g) Type / Format (unstructured data only)
h) External sharing (where the system allows):
    - What was shared
    - What organisation it was shared with (not individual)
    - When it was shared (includes when it is/was received)
i) Disposal trigger date (where the system allows, Information Group to advise)

Minimum audit metadata to assign when managing information:

j) Any later interaction with the information e.g., accessing, sharing, or modifying:
    - User
    - Date of action
    - Action taken

Minimum metadata to capture when disposing of information:

k) Unique identifier e.g., Object ID
l) Name / Title
m) Date created (or collected)
n) Business activity documented (which might be adequately described by the Disposal Class)
o) Creator e.g., individual and/or entity or system
p) Date of disposal
q) Disposal Action (e.g. Delete or Transfer)
r) Authority governing the disposal
s) Person or role or system carrying out the disposal action

3.1.7 When information is destroyed the System Owner ***must*** ensure that audit and disposal metadata is retained and either assigned to a stub, captured in a discoverable read-only log, or through another mechanism as approved by the Information Group.

3.1.8 The System Owner ***must*** ensure this standard is upheld to information in their repository.

3.1.9 The System Owner ***must*** ensure read-only metadata cannot be altered.

3.1.10 A copy of the metadata schema ***must*** be documented in an approved MSD repository other than the system it is describing so it is possible to verify that metadata fields are used in the way they were intended and aligned to the schema.

3.1.11 Any metadata settings and setting changes ***must*** only be implemented if approved by the Information Asset Owner and the System Owner with advice from the Information Group. The System Owner ***must*** ensure the agreed settings are implemented.

4 Standard Compliance

4.1 Exceptions

4.1.1 If any requirements from this standard cannot be met, then an exception must be granted, or the non-compliant activity stopped.

4.1.2 Exceptions ***must*** be applied for using the approved exceptions process.

4.2 Compliance Measurement

4.2.1 Compliance to this standard will be measured through various methods, including but not limited to monitoring, business tool reporting, internal and external audits, reviewing system configuration documentation and consultation with information asset owners and system owners.

4.3 Non-compliance

4.3.1 Any employee found to have violated this standard MAY be subject to disciplinary action as per the Ministry's Human Resources (HR) policies. This could include formal reprimands up to and including termination of employment.

5 Revision History

Date of Change	Responsible	Summary of Change
June 2024	Tallulah Willis	Aligning with updates to Archives New Zealand's current minimum metadata requirements, changes to requirements for read-only and disposal metadata to align with how the Ministry's environment operates in practice.

6 Definitions

Word / Phrase	Definition
Approved repository	A repository approved by MSD that meets business, legislative and information requirements.
Audit Metadata	Audit metadata captures details of interactions with information, such as access or modification. It should be read-only.
Dataset	A collection of structured data. Can also contain embedded unstructured data.
Disposal Action	Processes associated with implementing information destruction or transfer which are documented within disposal authorities and can only be applied by the Information Group. Transfer refers to the transfer of control of information to Archives New Zealand, or an authorised party.
Disposal Authority (DA) &	An information management instrument that defines the disposal actions that are authorised for specified records and can only be applied by the Information Group.

General Disposal Authority (GDA)	• General Disposal Authorities • GDA6 Common corporate service public records • GDA7 Facilitative, transitory, and/or short-term value records • MSD's current Disposal Authority (DA694)
Information	Recorded data or information in any form or medium, created or received and maintained as evidence of Ministry business (including processes, advice, activities, and decision-making). This includes, but is not limited to, documents, signatures, text, images, sound, speech or data and can come in a variety of formats such as electronic and paper files, email correspondence, film, tape, computer discs, text messages, social media, and web pages.
Information Asset	An Information Asset is an identifiable collection of data or information recognised as having value to the agency. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Asset Owner	All Information Asset Owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored. The Information Asset Owner must be someone who understands the value of the asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information. At MSD, Information Asset Owners will typically be DCE, Regional Commissioners or Group General Managers.
Metadata	Metadata is descriptive information e.g. the name, creator, creation date etc. It helps people to find, understand, authenticate, trust, use and manage information assets. Can be user or system generated.
Metadata schema	Logical plan showing the relationships between metadata elements, normally through establishing rules for the use and management of metadata.
System Owner	A Systems Owner is responsible for the overall operational and maintenance of a system where information is held, including any related support service, and ensuring all governance processes are followed and business requirements are met.

7 Related Standards

Standard	Purpose	Link
Information Retention and Disposal Standard	A metadata record must be retained when information is disposed.	Information Retention and Disposal Standard
Information Classification Standard	Classification metadata must be in line with the PSR security classifications as required by the Information Classification Standard.	Information Classification Standard
Information Migration Standard	Metadata must remain attached when information undergoes migration and unique identifiers must remain reconcilable across systems.	Information Migration Standard

8 References

Information Governance Policy

Archives New Zealand Metadata for information and records

Archives New Zealand Information and records management standard

Archives New Zealand General Disposal Authorities

Information Retention and Disposal Standard

Approved by:	Director, Information Foundations – Fiona McElwee on 14/04/2025
Standard Owner:	General Manager Information
Next Review Date:	April 2027
Review Committee	Information Policies and Standards Working Group

1 Purpose

This standard describes the Ministry of Social Development (the Ministry) expectations and requirements for the retention and disposal of information. Information retention and disposal are fundamental activities in an information asset's lifecycle. They enable the Ministry to appropriately manage information from creation to disposal. The Public Records Act 2005 sets obligations for how information created and received by public offices must be managed and disposed.

This standard supports and enables the principles in the Information Governance Policy that describe how the Ministry manages information assets in accordance with legislative requirements and how information assets held by the Ministry have responsible owners to ensure they are managed appropriately. Taking an active approach to managing information helps to ensure the Ministry has quality information to inform decision-making whilst also complying with legislative requirements.

2 Scope

This standard applies to all Ministry information created and collected for Ministry business that is subject to the Public Records Act 2005.

Definitions can be found at the bottom of this standard.

3 Standard

3.1 Retention and Storage

3.1.1 All Ministry information ***must*** be stored (digital information) or tracked (physical information) in the appropriate system, approved to hold such information[1], so it is protected and can be managed through its lifecycle.

3.1.2 System Owners are accountable for information in their systems. If a System Owner discovers that an information asset has been corrupted or otherwise made unavailable, they ***must*** immediately contact the Information, Privacy and Security Group (IPS) to determine the appropriate recovery or disposal action.

[1] The Certification and Accreditation Standard describes how the C&A process establishes what information a system is approved to hold.

3.2 Appraisal and Sentencing

3.2.1 Information Asset Owners ***must*** work with IPS to ensure that disposal can be completed routinely and systematically for their information assets beginning from the appraisal process.

3.2.2 Information ***must*** be appraised and sentenced in reference to relevant Disposal Authorities (DA) and General Disposal Authorities (GDA) by IPS to determine eligibility ***prior*** to any disposal activity. This can be carried out as part of system design or, where that is not possible, as the first step in a disposal process.

3.2.3 Appraisal ***must*** be carried out in consultation with the Information Asset Owner and any relevant System Owners and documented by IPS.

3.2.4 Where an appropriate Information Asset Owner cannot be identified, the General Manager Information will assume this role as required by IPS.

3.3 Approving Disposal

3.3.1 Any disposal actions ***must*** be approved by the relevant Information Asset Owner before implementation.

3.3.2 Any disposal actions other than routine disposal ***must*** be authorised by IPS on a case-by-case basis before implementation to ensure that relevant parties have been engaged, and that the appropriate Disposal Authority has been identified and documented.

3.3.3 The Information Asset Owner ***must*** notify IPS on completion of approved non-routine disposal actions so IPS can update the Information Asset Register.

3.4 System Requirements

3.4.1 Systems holding Ministry information ***must*** protect the information to maintain its:

- integrity (information is protected against unauthorised modification and corruption);
- availability (information is usable and in an appropriate format); and
- confidentiality (information can be accessed only by approved parties for specific purposes).

3.4.2 The Information Asset Owner ***must*** work with IPS and the System Owner to establish:

- metadata settings[2] for their information assets (e.g., frequency of disposal, triggers); and
- system settings to allow that metadata to be used as part of routine disposal.

3.4.3 The System Owner ***must*** ensure that these settings (including any routine disposal processes) are implemented as approved by IPS.

3.4.4 The System Owner ***must*** ensure routine disposal occurs according to these settings. Systems ***must*** permanently destroy information when it is disposed so it cannot be recovered for ongoing use by the business.

3.4.5 Systems ***must*** generate metadata records as appropriate to record disposal actions[2]. If a metadata record cannot be retained within the system, the System Owner ***must*** contact ISI for advice.

[2] See the Minimum Metadata Capture Standard for metadata requirements.

4 Standard Compliance

4.1 Exceptions

4.1.1 If one or more requirements from this standard cannot be met, the Information Asset Owner and/or System Owner ***must*** apply for an exception to the standard.

4.1.2 Exceptions ***must*** be applied for using the approved exceptions process.

4.2 Compliance Measurement

4.2.1 The Standard Owner will verify compliance to this standard through various methods, including but not limited to, monitoring, business tool reporting, internal and external audits, documentation review and consultation with Information Asset Owners and System Owners.

4.3 Non-compliance

4.3.1 Any employee found to have violated this standard MAY be subject to disciplinary action as per the Ministry's Human Resources (HR) policies. This could include formal reprimands up to and including termination of employment.

5 Revision History

Date of Change	Responsible	Summary of Change
December 2024	Tallulah Willis	Administrative and minor technical changes to wording and structure, and aligning requirements with current Ministry practice.
July 2025	Tallulah Willis	Minor wording changes and including information retention and disposal process diagrams.

6 Definitions

Word / Phrase	Definition
Appraisal	The process of evaluating business activities. Includes analysis of business context, business activities and risk to enable decision making on what records to create and capture, and how to ensure the appropriate management of information over time. Appraisal can occur: • Before information and records' creation and during the design of business processes. • At creation — to ensure information and records are correctly managed over time. • Retrospectively — after information and records have fulfilled their immediate purpose. • When there is an administrative change or transfer of function.

Destruction	Process of eliminating or deleting information beyond any possible reconstruction.
Disposal Action	Processes associated with implementing information destruction or transfer which are documented within disposal authorities and can only be applied by the Information, Privacy and Security Group. Transfer refers to the transfer of control of information to Archives New Zealand, or an authorised third party.
Disposal Authority (DA) & General Disposal Authority (GDA)	An information management instrument that defines the disposal actions that are authorised for specified records and can only be applied by the Information, Privacy and Security Group. • General Disposal Authorities • GDA6 Common corporate service public records • GDA7 Facilitative, transitory, and/or short-term value records • MSD's current Disposal Authority (DA694)
Information	Recorded data or information in any form or medium, created or received and maintained as evidence of Ministry business (including processes, advice, activities, and decision-making). This includes, but is not limited to, documents, signatures, text, images, sound, speech or data and can come in a variety of formats such as electronic and paper files, email correspondence, film, tape, computer discs, text messages, social media, and web pages.
Information Asset	An Information Asset is an identifiable collection of data or information recognised as having value to the agency. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Asset Owner	All Information Asset Owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored. The Information Asset Owner must be someone who understands the value of the asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information. At MSD, Information Asset Owners will typically be DCE, Regional Commissioners, General Managers or Group General Managers.
Metadata	Metadata is descriptive information, e.g., The name, creator, creation date, etc. It helps people to find, understand, authenticate, trust, use and manage information assets. Can be user or system generated.
Routine Disposal	Routine disposal refers to disposal actions that occur on a regular basis according to pre-agreed rules or settings, e.g., those implemented into a system or described in an operational process or standard.
Sentencing	Sentencing is the process of applying Disposal Authorities to information assets that have been appraised to identify the minimum retention periods and disposal actions for those information assets, thereby enabling appropriate decisions to be made about how the information is managed through to disposal.
System Owner	A System Owner is responsible for the overall operational and maintenance of a system where information is held, including any related support service, and ensuring all governance processes are followed and business requirements are met.

7 Related Standards

Standard	Purpose	Link
Minimum Metadata Capture Standard	Metadata is required to manage information assets and a metadata record must be captured when information is disposed.	Minimum Metadata Standard
Information Classification Standard	System settings must manage access to classified information according to the Information Classification Standard.	Information Classification Standard

8 References

Public Records Act 2005

Archives New Zealand General Disposal Authorities

Ministry of Social Development Disposal Authority

Information Governance Policy

Minimum Metadata Capture Standard

Protective Security Requirements

Information Classification Standard

9 Appendix: Information Retention and Disposal Process Diagrams

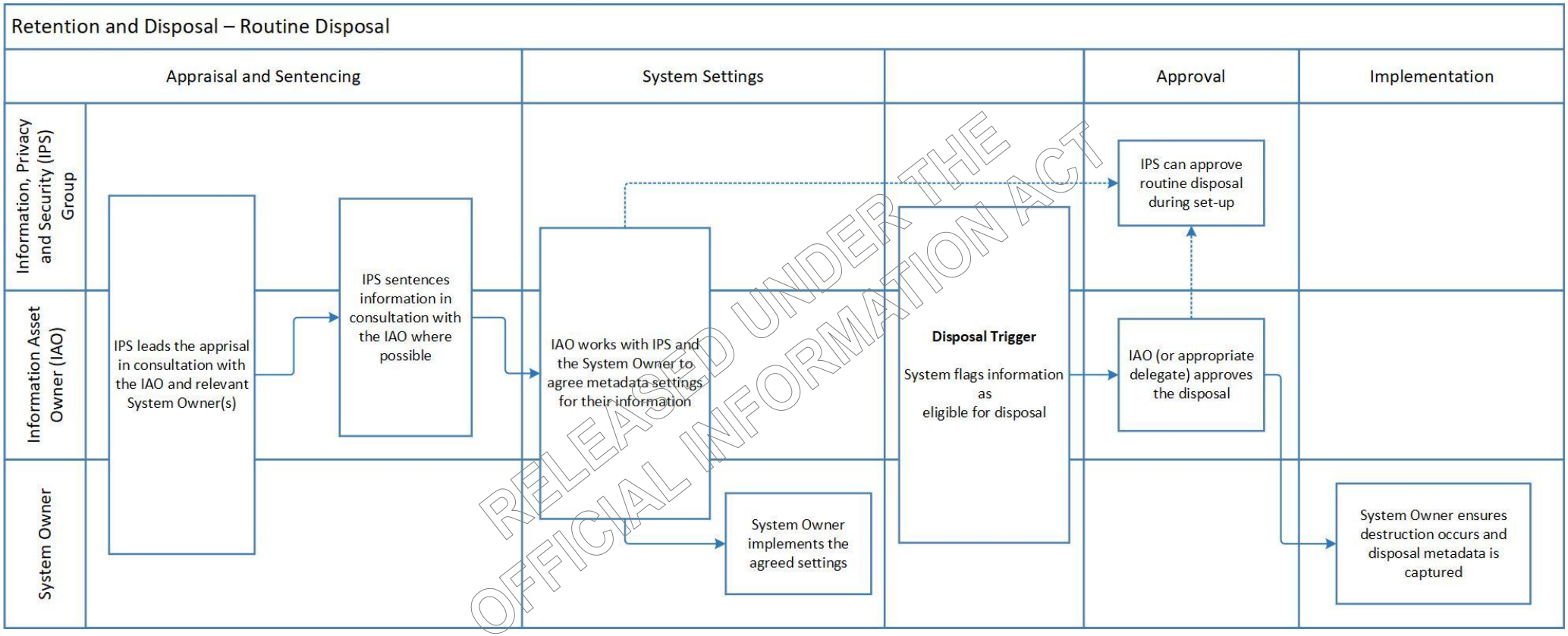


Figure 1: Routine disposal process.

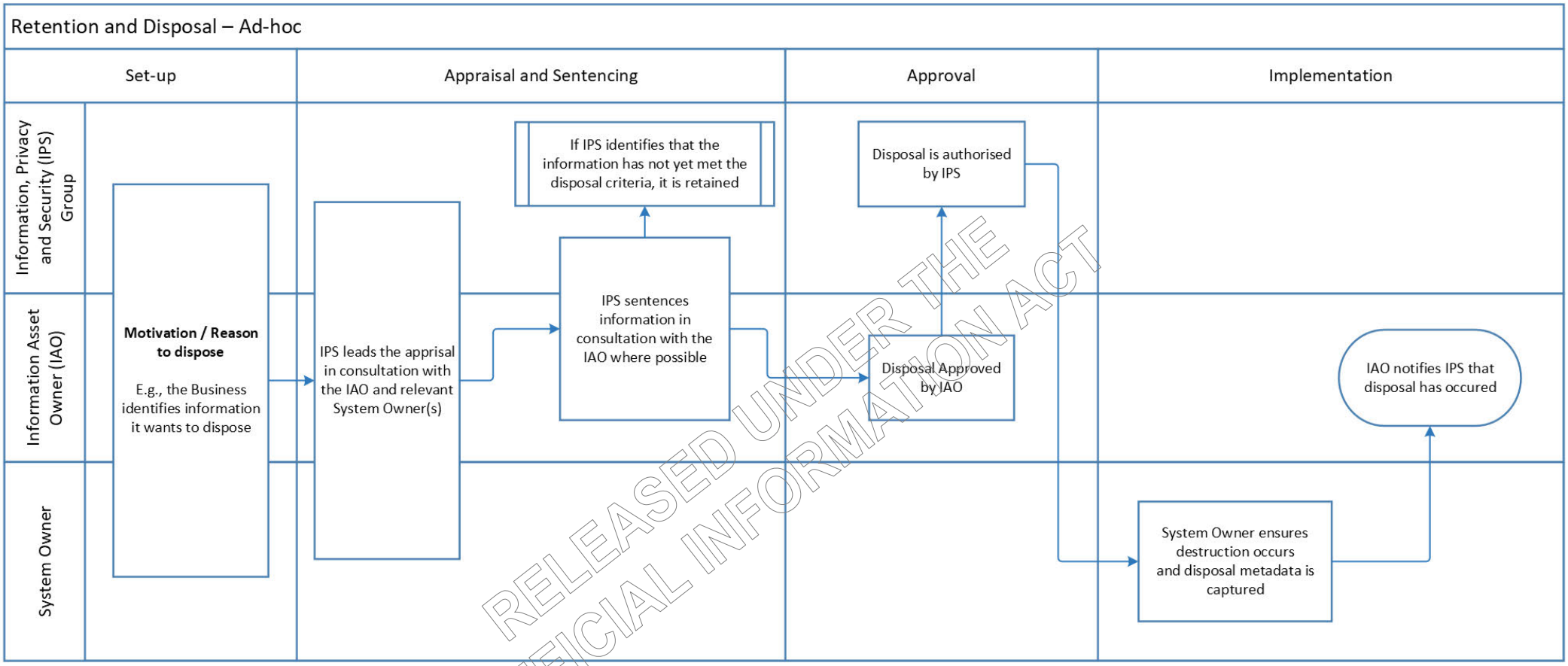


Figure 2: Ad-hoc disposal process.

Information Migration Standard

Approved by:	Fiona McElwee, Director Information Policy, Capability and Operations on 31 October 2025
Standard Owner:	General Manager Information
Next Review Date:	October 2027
Review Committee	Information Policies and Standards Working Group

1 Purpose

This standard describes the Ministry of Social Development's (the Ministry) expectations and requirements when migrating information. This standard also describes the responsibilities of Information Asset Owners when executing migrations to ensure information subject to migration is properly managed and protected.

This standard applies to all information created, stored, and collected by or on behalf of the Ministry, which is subject to the Public Records Act 2005. This standard also outlines the Ministry's obligations to meet the Archives New Zealand Information and Records Management Standard.

- The standard supports and enables following principles in the Information Governance Policy.
- The Ministry's information assets are identified and appropriately protected based on legislative requirements, information value and risk culture
- Information assets are fit-for-purpose to promote informed decision-making.

2 Scope

This standard covers any migration of information where the Ministry has a direct responsibility (and is accountable for) managing information in a safe, secure and trustworthy way. The Third Party Provider Information Assurance Standard both defines what direct responsibility is and sets out several examples where this can occur. This Information Migration Standard therefore applies to systems that contain Ministry information, or information about Ministry staff or clients, regardless of where those systems are located. Examples include:

- Migration from one system to another (new system; system that has never housed this information before).
- Migration as part of a function transfer
- Repatriation of information (external vendor system that is no longer viable).

Migration of information where the Ministry has no responsibility, or an indirect responsibility (as defined in the Third Party Provider Information Assurance Standard), for managing information is out of scope.

Definitions can be found at the bottom of this standard.

3 Migration Principles

These principles are set to support pragmatic decision-making about the migration of information and data.

PRINCIPLE	Description
Only take quality information	Quality information supports good decision-making. It is trusted and can be easily accessed and used by the people who need it. Quality information: • Has context and is described properly, • Has a valid file type with a known application, and • Has an identified Business Owner.
Only take information with confirmed business value	By taking as little information as possible, we ensure the information we migrate will be more discoverable. With a lower volume of information being migrated, migrations will be completed faster and with fewer errors. Business Owners are required to confirm whether information they are responsible for: • Is actively used and aligned to a current function, and • Is required for compliance but either hasn't met the disposal trigger date or is required to be transferred to Archives New Zealand under a Disposal Authority (GDA 6 or DA694). Information that is not actively used and has met its disposal trigger can be destroyed at the discretion of the General Manager Information.
Business value is determined by owner	The Information, Privacy and Security Group (IPS) defers to the business on what is of value and what is required to deliver their function. • Decisions to dispose rest with the business. • Where the Information Asset Owner cannot be identified, ownership is transferred to the General Manager Information.
Match destination systems to business need	The destination system must be fit for purpose for how the information will be used. • Active and archive locations are chosen based on understood business needs. • Exclude information assets that belong in specific line of business system.

4 Standard

4.1.1 The Information Asset Owner ***must*** ensure the purpose of migration and details of the information in scope are defined and documented.

4.1.2 The Information Asset Owner and System Owner(s) ***must*** also identify the following attributes to enable the information risks to be properly identified:

- Volumes (size, quantity)
- Format (file type, structured or unstructured)
- Age (date range)
- Function (business purpose or use).

4.1.3 Solution design for the destination system within the Ministry ***must*** be documented, where information is migrated to new systems or ones that have not housed this information before.

4.1.4 The System Owner(s) ***must*** ensure that the destination system has been risk assessed, certified by the General Manager Information, and accredited by the responsible Deputy Chief Executive before go-live.

4.1.5 Systems Owner(s) ***must*** ensure the destination system meets the requirements of the Minimum Metadata Capture Standard.

4.1.6 When a migration is required due to a legislated change in agency responsibilities, the Function Transfer Standard also applies as described under Section 23 of the Public Records Act 2005.

4.1.7 All migration activities ***must*** be documented in a migration plan (refer to appendix A for a sample template) in consultation with the Information Asset Owner, System Owner(s) and IPS so that it can be risk assessed. These activities ***must*** include:

- Scope of migration
- Destination state
- Description of migration mechanisms and phases
- Migration testing
- Disposal activities (if applicable).

4.1.8 Information in scope for migration ***must*** be assessed by IPS before migration activities occur to confirm whether it should be disposed instead of being migrated. For any disposal activity, the Information Retention and Disposal Standard applies.

4.1.9 Success criteria for migration ***must*** be documented in the migration plan. This success criteria ***must*** also include an acceptable failure rate, informed by testing and at a level approved by IPS.

4.1.10 Any proposed data transformation or cleansing activities ***must*** be documented and ***must*** only be included into the migration plan if agreed to by IPS.

4.1.11 IPS ***must*** be notified after migration is complete to confirm success criteria has been met and to record any disposal activities in the destruction register.

5 Standard Compliance

5.1 Exceptions

5.1.1 If one or more requirements from this standard cannot be met, the System Owner or Information Asset Owner must apply for an exception to the standard.

5.1.2 Exceptions ***must*** be applied for using the approved exceptions process.

5.2 Compliance Measurement

5.2.1 The General Manager Information will verify compliance to this standard through various methods, including but not limited to, periodic walk-throughs, internal and external audits, feedback to the policy owner and confirmation through the migration plan.

5.3 Non-compliance

5.3.1 Any employee found to have violated this standard MAY be subject to disciplinary action as per the Ministry's Human Resources (HR) policies. This could include formal reprimands up to and including termination of employment.

6 Revision History

Date of Change	Responsible	Summary of Change
09 / 2023	Nikhita Mistry	New standard developed.
10/2025	Tallulah Willis	Minor wording changes.

7 Definitions

Word / Phrase	Definition
Direct responsibility	Holds the information within its own systems. Uses an external service provider, such as a cloud service provider, to store, process or use information on behalf of MSD or otherwise in accordance with MSD's instructions. During the sharing process when information is shared between MSD and the third party. Where a service or product that collects, uses, stores or shares information is co-developed or co-delivered with, or co-branded by MSD, for example, a joint agency solution or a private/public initiative.
Information	Recorded data or information in any form or medium, created or received and maintained as evidence of Ministry business (including processes, advice, activities, and decision-making). This includes, but is not limited to, documents, signatures, text, images, sound, speech or data and can come in a variety of formats such as electronic and paper files, email correspondence, film, tape, computer discs, text messages, social media, and web pages.
Information Asset Owner	All Information Assets Owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored. The Information Asset Owner must be someone who understands the value of the asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information. At MSD, Information Asset Owners will typically be DCE, Regional Commissioners, Group General Managers or General Managers.
Migration	Migration is the process of transferring information from one system or application to another, including its metadata.
Migration activities	Specific processes and / or tools used to move data and information to one location to another.
Migration Plan	Refer to Migration Plan template (appendix A).
System Owner	A System Owner is responsible for the overall operational and maintenance of a system where information is held, including any related support service, and ensuring all governance processes are followed and business requirements are met.

8 Related Standards

Standard	Purpose	Link

Function Transfer Standard	This standard applies when the information relating to a business function is being moved from one organisation to another.	Function Transfer Standard
Third Party Information Assurance Standard	This standard must be applied when MSD engages, funds or collaborates with a third party to provide services or products and it involves the collection, use, storage, sharing or disposal of information.	Third Party Information Assurance Standard
Information Retention and Disposal Standard	This standard applies to the changing statuses during information's lifecycle (i.e., creation, use, change and ultimately disposal).	Information Retention and Disposal Standard
Minimum Metadata Capture Standard	This standard applies to MSD information assets covered by relevant Disposal Authorities (DA) and "Archives New Zealand's General Disposal Authority (GDA) - 6 Common corporate service public records", but not "General Disposal Authority (GDA) 7 Facilitative, transitory, and/or short-term value records".	Minimum Metadata Capture Standard
Information Classification	This standard applies to information created or received by MSD. Classification of information that is stored internally must be treated as IN-CONFIDENCE until reclassified.	Information Classification Standard

9 Appendices

The following Appendices are pertinent to this standard:

- Appendix A: Migration Plan template

Appendix A: Migration Plan template

9.1.1 Information and Data Migration Plan

Project / Initiative (if applicable)	
Team / Business Group	
Key contact	
Date	

Introduction
• Project overview and background • Solution Design • Description of current system(s) • Description of destination system(s)

High-Level Summary
• High level scope • Data to migrate • Data not migrated

Migration approach
• Description of dependencies or prerequisites • Description of mechanisms • Timelines (phases and key dates) • Data mapping • Transformation (detailed processes) • Cleansing activities (detailed processes) • Migration activities (detailed processes) • Testing activities • Success criteria • Rollback • Remediation (including post migration fixes)

Data destruction and decommissioning (if applicable)
• Description of dependencies or prerequisites • Timelines (phases and key dates) • Destruction/decommission activities (detailed processes)

Completed by	
Date	
Reviewed / Endorsed by (if applicable)	

Date	

Information Classification Standard

Approved by:	General Manager Information Group, Hannah Morgan on 09/07/2024
Standard Owner:	General Manager Information Group
Next Review Date:	July 2026
Review Committee	Information Policies and Standards Working Group

1 Purpose

This standard describes the Ministry of Social Development (the Ministry) expectations and requirements for information classification. It describes the responsibilities of Ministry staff when classifying information and using classified information to ensure it is properly managed and protected, and the requirements for Ministry systems when holding and processing classified information.

Our Information Governance Policy defines how the Ministry's information assets are identified and appropriately protected based on legislative requirements[1], information value and the Ministry's risk culture. Our Information Security Policy requires that the Ministry must protect its information assets through right-sized security controls. This standard supports these requirements through ensuring that information is classified, allowing its risk to be understood.

2 Scope

This standard applies to all information created, stored, and collected by or on behalf of the Ministry, which is subject to the Public Records Act 2005.

This standard applies to employees, contractors, consultants, temporaries, and other workers at the Ministry including all personnel affiliated with third parties.

Definitions can be found at the bottom of this standard.

[1] The Classification System Policy created by the Protective Security Requirements outlines the mandatory use of this system within government departments.

3 Standard

3.1 Classifications

3.1.1 All information created or received by the Ministry ***must*** be assigned a security classification as described by the Protective Security Requirements (PSR).

3.1.2 Ministry systems ***must*** only hold information classified up to RESTRICTED.

3.1.3 Any information with NEW ZEALAND EYES ONLY (NZEO) and ACCOUNTABLE MATERIAL markings ***must*** be rejected from systems that interface with SEEMail without storing or processing the information.

3.1.4 Where information has not been classified it ***must*** be managed in line with the requirements for IN CONFIDENCE.

3.1.5 Information classified as IN CONFIDENCE, SENSITIVE or RESTRICTED ***must*** be managed in line with the Ministry's information classification guidance.

3.1.6 All information must have a clearly visible classification and endorsement marking applied.

3.2 IN CONFIDENCE

3.2.1 IN CONFIDENCE classified information can be shared with all Ministry employees, other New Zealand government agencies and authorised 3rd parties, but ***must not*** be shared publicly.

3.3 SENSITIVE and RESTRICTED

3.3.1 SENSITIVE and RESTRICTED classified information ***must*** only be shared with Ministry employees, other New Zealand government agencies and authorised 3rd parties that need access for the purposes of their role within the Ministry or as required by a contract, information sharing agreement, legislation or similar authority.

3.3.2 All systems processing and holding SENSITIVE and RESTRICTED information ***must***:

- Have an access model based on user roles or attributes, with defined permissions for granting access to information.
- Require access to information classified as SENSITIVE or RESTRICTED (or areas of the system containing that information) to be granted only as described in that access model.

3.4 Reclassification

3.4.1 Information ***must*** be reclassified when the risk of compromising that information changes, e.g. when an IN CONFIDENCE classified document is authorised to be published, it should be marked as unclassified, or when a person's circumstances change and their information held by the Ministry could endanger their safety, that information should be reclassified from IN CONFIDENCE to SENSITIVE.

3.4.2 Information ***must not*** be reclassified without approval by the Information Asset Owner or their delegate. Information received from another agency is owned by that agency for this purpose.

3.4.3 Information classified under another system that is received by the Ministry ***must*** be assigned an equivalent PSR classification in consultation with the Information Group, e.g., information classified in Australia that is received by the Ministry will require an equivalent PSR classification.

4 Standard Compliance

4.1 Exceptions

4.1.1 If any requirements from this standard cannot be met, then an exception must be granted, or the non-compliant activity stopped.

4.1.2 Exceptions ***must*** be applied for using the approved exceptions process.

4.2 Compliance Measurement

4.2.1 CISO ***must*** verify compliance with this standard through the Certification and Accreditation process by assessing the information against this standard and ensuring appropriate mechanisms are in place.

4.3 Non-compliance

4.3.1 Any employee found to have violated this standard MAY be subject to disciplinary action as per the Ministry's Human Resources (HR) policies. This could include formal reprimands up to and including termination of employment.

5 Revision History

Date of Change	Responsible	Summary of Change
June 2024	Tallulah Willis	Removal of cross-referencing of other standards, inclusion of requirement to apply a PSR classification to information classified overseas, changes to align with how the Ministry's environment operates in practice.

6 Definitions

Word / Phrase	Definition
Information	Recorded information (including data) in any form created or received and maintained as evidence of Ministry business. It includes, but is not limited to, documents, email correspondence, datasets, audit logs, text messages, voice recordings, social media, and web pages.
Information Asset Owner	All Information Assets Owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored. The Information Asset Owner must be someone who understands the value of the asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information. At MSD, Information Asset Owners will typically be DCE, Regional Commissioners or Group General Managers.
MSD System	Any systems, on-premises and in the cloud, network assets, and computing devices used to conduct MSD business or interact with internal/external networks and business systems, whether owned by MSD, the employee or a third party.

System Owner	A System Owner is responsible for the overall operation and maintenance of a system where information is held, including any related support service, and ensuring all governance processes are followed and business requirements are met.

7 Related Standards

Standard	Purpose	Link
Authentication Standard	Users accessing classified information in a Ministry system must be authenticated.	Authentication Standard
Encryption Standard	Information classified as IN CONFIDENCE or above must be encrypted in transit and at rest.	Encryption Standard
Information Retention and Disposal Standard	Classified information must be disposed in line with the Information Retention and Disposal Standard.	Information Retention and Disposal Standard
Minimum Metadata Capture Standard	Information classification metadata is required to meet the Minimum Metadata Capture Standard.	Minimum Metadata Capture Standard

8 References

Information Governance Policy

Information Security Policy

Protective Security Requirements

NZISM

Guidelines for Protection of Official Information

Guidelines for handling SENSITIVE and RESTRICTED documents and material