MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

29 April 2026

Tēnā koe

Official Information Act request

Thank you for your email of 12 February 2026, to the Ministry of Social Development (the Ministry), requesting policies and risk assessments regarding governance and protection of mātauranga Māori and Māori data sovereignty.

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

Part 1: Tiriti-Based Policy and Governance Frameworks
Please provide all and any documentation that outlines your organisation's approach to:

1. *The governance and protection of mātauranga Māori and Māori data (especially as a taonga), and the implementation of the principles of Māori Data Sovereignty.*

Information in scope of this part of your request has previously been released in another request. I recommend you visit the following link which provides the information: www.msd.govt.nz/documents/about-msd-and-our-work/publications-resources/official-information-responses/2025/march/06032025-maori-data-sovereignty-and-maori-data-governance.pdf.

I have identified one other documents in scope of the above part of your request. I have enclosed a copy of the Ministry's Data Jurisdiction Standard with this letter.

2. *How your organisation gives effect to the Waitangi Tribunal's findings in Wai 262 and Wai 2522 regarding the Crown's duty of active protection and the guarantee of tino rangatiratanga over these taonga.*

The Ministry has not specifically considered the implications from the Waitangi Tribunal's finding however we continue to follow all of government advice that may have accounted for this, such as Archives New Zealand.

I am therefore refusing the above part of your request under section 18(e) of the Act as the information requested does not exist.

3. *Specific policies governing the digitisation of mātauranga Māori (including physical taonga and oral records) and the management of resulting digital assets.*

I have identified the Ministry's Digital Information Standard to be in scope of this part of your request. The Digital Information Standard describes the Ministry's expectations around digital information, including digitisation. I have enclosed a copy of this with this letter.

Part 2: Risk Assessments and Threat Mitigation
Please provide:

1. *Any risk assessments conducted since 2020 that specifically evaluate threats to mātauranga Māori and Māori data, including from:*
    - *Automated web scraping for AI training datasets.*
    - *The use of cloud and AI services provided by third parties (e.g. Microsoft, Google, Amazon, OpenAI).*
    - *The "digital colonialism" or unauthorised commercial exploitation of this taonga.*
2. *All documents (briefings, reports, memos) that discuss the risks identified in the above assessments and propose or detail mitigation strategies.*

The Ministry has not conducted any risk assessments that are in scope of your request. Therefore, I am refusing the above parts of your request under section 18(e) of the Act as the information requested does not exist.

Part 3: Third-Party Agreements and Technical Safeguards
Please provide:

1. *Copies of any current agreements, contracts, or data sharing addenda with cloud storage or AI technology providers (e.g. Microsoft, Google, Amazon Web Services, OpenAI). I specifically seek any and all clauses within these documents that relate to:*
    - *Data sovereignty and the geographic location/storage of data.*
    - *The use of customer data for the training or improvement of the provider's AI models.*
    - *The protection of Indigenous data or cultural heritage.*
    - *Any explicit recognition of Te Tiriti o Waitangi or Māori Data Governance.*

I have identified the Microsoft Cloud, Software and Services Agreement (MCSSA) to be in scope of this part of your request. The MCSSA is an all-of-government Microsoft volume licensing agreement that includes subscription-based, perpetual and cloud services licensing.

The Department of Internal Affairs (DIA) is the lead agency for this agreement. Ordinarily the Ministry would be required to transfer your request to DIA for response. However, I understand you have also made the same request to DIA. In this case, I have not transferred this part of your request.

Additionally the Terms of Service for the Google Services are publicly available at the following links:

- Google Cloud Terms of Service can be found at: https://workspace.google.com/terms/premier_terms/.

- Google Cloud Terms of Service can be found at: https://cloud.google.com/terms.
- Google APIs Terms of Service can be found at: https://developers.google.com/terms.

Please note, this part of your request also encompasses additional Cloud Services Agreements. However, in order to provide you with information on specific clauses from these agreements, the Ministry would need to divert personnel from their core duties and allocate extra time to complete this task. The diversion of these resources would impair the Ministry's ability to continue standard operations and would be an inefficient use of the Ministry's resources. As such, your request is refused under section 18(f) of the Act, as it requires substantial collation. The greater public interest is in the effective and efficient administration of the public service.

I have considered whether the Ministry would be able to respond to your requests given extra time, or the ability to charge for the information requested. I have concluded that, in either case, the Ministry's ability to undertake its work would still be prejudiced.

2. *Documentation detailing the technical measures in place to prevent the automated scraping of mātauranga Māori from your public-facing websites and digital repositories. This includes, but is not limited to API access controls, rate limiting, and any other technical barriers.*

I am refusing the above part of your request under section 18(e) of the Act as the information requested does not exist.

Part 4: Resourcing for Active Protection
Please provide any documentation that outlines the budgeting, business planning, and resourcing (e.g. Full-Time Equivalent staff, specific project funding) allocated to:

1. *Give effect to the policies and frameworks mentioned in Part 1.*
3. *Specifically, any business cases or budget requests that were made to address the threats posed by AI and were either approved or declined.*

I am refusing the above parts of your request under section 18(e) of the Act as the information requested does not exist.

2. *Implement the mitigation strategies identified in Part 2.*

The Ministry has one dedicated FTE focussed on Māori data practices: Senior Analyst, Māori Data & Insights.

Beyond this role, other staff contribute to Māori data practices in meaningful ways as part of their broader responsibilities, but it is not possible to quantify their time as a nominal FTE allocation.

Note that while the previous request (referenced in part one) also included a Principal Māori Data Governance Advisor role, this was a fixed term position which has now ended.

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

DATA JURISDICTION STANDARD

Approved by:	Chief Information Security Officer (CISO) – Hannah Morgan on 19/12/2023
Standard Owner:	Chief Information Security Officer (CISO)
Next Review Date:	December – 2025

1 Purpose

The Ministry of Social Development ("MSD") has a legal and ethical obligation to safeguard the data that we collect. This includes MSD data and the data of New Zealanders, including Māori.

Data stored in, or traversing through, cloud computing services may be under the jurisdiction of more than one country's laws and complying with New Zealand laws and regulations alone may not be sufficient. There are different legal requirements regarding data security, privacy, and breach notification that could apply, depending on where the data is being hosted, accessed from, or who is controlling it.

With the MSD's increasing uptake of cloud computing and remote access, we must ensure that we know precisely where MSD data and the data of our clients is held, or accessed from, at any given time in the data lifecycle. This is to ensure we adequately protect the data and comply with all applicable local data laws and regulations.

This Standard describes the:

- jurisdictions currently approved to hold MSD and client data;
- countries that MSD staff are allowed to access MSD Systems from;
- requirements to assess approved and additional jurisdictions, including monitoring requirements for jurisdictional changes;
- minimum documentation requirements including data flows; and
- handling of exceptions to this Standard.

Applying this Standard will ensure jurisdictional, sovereignty and privacy risks are fully considered and formally accepted.

2 Scope

This Standard is linked to the Information Security Policy and the Remote Access Standard[1] and ensures that MSD protects data through right-sized security controls and that access to and use of MSD data is only available to those that need it to perform their role.

Both Standards must be applied to all third parties engaged with MSD to store, process, transmit, or access MSD data, and any personnel accessing MSD Systems and data from overseas.

Definitions can be found at the bottom of this Standard.

[1] The Remote Access Standard applies to all MSD users who undertake work for or on behalf of MSD (e.g., MSD Staff) and access MSD Systems remotely (i.e., not from an MSD office).

3 Standard

3.1 Jurisdictions – Cloud Service Providers

3.1.1 New Zealand based services that host data in New Zealand **must** be considered first, followed by services that are hosted in Australia.

3.1.2 If a service is considered that is based outside of New Zealand or Australia and/or that hosts data in jurisdictions other than New Zealand or Australia:

- a rationale **must** be documented as to why a New Zealand/Australia based service cannot be used; and
- documentation, for example a data flow diagram, **must** be prepared to record all data flows and storages, and the applicable jurisdictions.

3.1.3 Any jurisdiction outside of New Zealand or Australia **should** be assessed using the DPMC Jurisdiction Assessment Framework and the Protective Security Requirements (PSR)[2].

3.1.4 Services from countries assessed as high risk using the DPMC Assessment Framework and the PSR **must not** be used.

3.1.5 Services from countries assessed as medium risk using the DPMC Assessment Framework and the PSR **may be** approved but **must** undergo a detailed risk assessment, and sufficient controls **must** be in place to mitigate the risk to low in accordance with the DPMC Assessment Framework and the PSR.

3.1.6 Offshore services **must not** be used for storing or processing data protectively marked CONFIDENTIAL, SECRET, or TOP SECRET.

3.1.7 If a service is based outside of New Zealand and is responsible for handling or storing personal and identifiable information, the potential impacts to Māori **should** be documented.

3.1.8 As per 3.1.2., all data processing, transit, access and at rest **must** be documented and show all data flows and storage locations, and the applicable jurisdictions data flows through, or is stored in.

3.1.9 Documentation **must** include all Systems, including production and non-production Systems and data backups, and any disaster recovery environments.

3.1.10 An exit strategy for the service **must** be documented and the strategy **must** cover:

- trigger criteria;
- business impacts and risks;
- roles and responsibilities for exiting the service;
- timeframes for exiting the service;
- migrating data back to MSD prior to decommissioning the service;
- erasing data from the service on conclusion of service; and
- considerations for technical factors that would enable migration to another platform in the future (networking, management tools, integrations, third party services, data extraction, data destruction).

[2] The DPMC Jurisdiction Assessment Framework and PSR Guidance documents are classified as RESTRICTED and hence no details or references on what they assess and how have been included in this document.

3.2 Jurisdictions – People Accessing MSD Systems and Data from Overseas

3.2.1 Requests to access MSD Systems and data from overseas[3], irrespective of device, **must** be granted only in exceptional circumstances and only for work events and follow the Remote Access Standard[4].

> *Exceptional circumstances* means circumstances that could not be reasonably foreseen that require supporting critical MSD functions and that would, if not performed, cause adverse impacts to MSD's operations. For example, for the purpose of business continuity.
> **and**
> *Work events* means events that occur in connection with a person's employment such as attending conferences or delegations.

3.2.2 Access to MSD Systems and data from jurisdictions assessed as low risk using the DPMC Jurisdiction Assessment Framework and the PSR **must** be approved by the Remote Access Standard Owner.

3.2.3 Access to MSD Systems and data from jurisdictions assessed as medium or high risk using the DPMC Assessment Framework and the PSR **must** be approved by the Information and Protective Security Oversight Committee and the Remote Access Standard Owner.

3.2.4 Any requests for accessing MSD Systems or data from overseas, including their approvals, **must** be formally captured, and retained.

3.3 Jurisdictions – Assessment, Documentation Requirements and Monitoring

3.3.1 Any advisories published by the DPMC and the PSR **must** be reviewed and actioned as required.

3.3.2 Approved jurisdictions **must** be monitored for jurisdictional changes that could change the risk profile to MSD.

3.3.3 Jurisdictions approved by MSD outside of this Standard **must** be at least reviewed every two years to confirm that their risk profile has not changed.

3.3.4 Jurisdiction assessments and their review must be documented, and jurisdictional approvals captured in, an MSD-approved file repository that allows storage of data classified as RESTRICTED.

[3] Including countries written to include the Five Eyes Alliance, i.e., the United States, the United Kingdom, Canada, and Australia.

[4] Refer to the Remote Access Standard for the requirements of accessing MSD Systems and Information remotely either from New Zealand or as approved by MSD.

4 Roles and Responsibilities

Role	Responsibility
Chief Information Security Officer (CISO)	Sets the strategic direction for information security within MSD. 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 team through a distributed security function. At MSD, the Chief Executive has delegated the CISO role to the General Manager (GM) Information. The GM Information is responsible for implementing and having assurance over this Standard and for the review and approval of jurisdictional risk assessments and remote access requests
Organisational Health Committee (OHC)	The OHC is responsible for ensuring the overall integrity of MSD's operations by making sure there is ongoing compliance with legislation and policy, communication with the public and stakeholders is effective, and Ministers are supported.
Remote Access Standard Owner	The Remote Access Standard Owner is the IT Security Manager. At MSD, the CISO has delegated the ITSM role to the Director Technology Security and Identity. The Standard owner reviews and approves access requests, where required with the GM Information.
Information and Protective Security Oversight Committee (IPSOC)	The Information and Protective Security Oversight Committee is an enabling and assurance group for all MSD business groups to ensure the activities we engage in to support the work we do with clients is carried out in a way that keeps everyone safe and minimises risk to the organisation.

5 Standard Compliance

5.1 Exceptions

5.1.1 Exceptions **must** be requested from the Information and Protective Security Oversight Committee and include:

- A brief description of the System or service, or remote access use case, where standard requirements cannot be met;
- provide which standard requirement(s) cannot be met;
- explain why standard requirement(s) cannot be met; and
- the plans of service provider to achieve full compliance.

5.1.2 Exception requests to the Information and Protective Security Oversight Committee **must** include the:

- result of the jurisdictional risk assessment using the DPMC Jurisdiction Assessment Framework;
- rationale for why a low-risk jurisdiction cannot be used;
- proposed compensating Controls and the impact on the jurisdictional risk assessment;
- an assessment of the impact to Māori and Māori data sovereignty; and
- a description of how Māori have been consulted on the exception, and the outcome of this consultation.

5.1.3 The Information and Protective Security Oversight Committee **must**:

- approve the use of the jurisdiction if there are compensating Controls that reduce the risk to
- low; or
- refer the decision to the Organisational Health Committee if there is a medium or high risk for which there are no compensating Controls that can reduce the risk to low.

5.2 Compliance Measurement

5.2.1 The Chief Information Security Officer ("CISO") **must** verify compliance to this Standard. This can be through various methods, including but not limited to: Certification and Accreditation, periodic reviews, and internal and external audits.

5.3 Non-compliance

5.3.1 Any MSD Staff found to have violated this Standard may be subject to disciplinary action in accordance with MSD's Human Resources ("HR") manual. This could include formal reprimands up to, and including, termination of employment.

6 Revision History

Date of Change	Responsible	Summary of Change
December / 2020	Christopher Miller	Initial draft (approved by Privacy and Security Oversight Board on 14/12/2020)
June / 2021	Christopher Miller	Minor updates
December / 2023	Katja Feldtmann	Moved Standard to new MSD template; removed encryption section; added specific requirements for Cloud Service Providers and people accessing MSD Systems from overseas

7 Definitions

Word / Phrase	Definition
Accreditation	Accreditation is the formal authority to operate a system, evidence that governance requirements have been addressed and that the Chief Executive has fulfilled the requirement to manage risk on behalf of the organisation and stakeholders. Accreditation ensures that either sufficient security measures have been put in place to protect information that is processed, stored, or communicated by the system or that deficiencies in such measures have been identified, assessed, and acknowledged, including the acceptance of any residual risk.
Certification	Certification is the assertion that a System (including any related or support services such as telecommunications or cloud) complies with the minimum standards and Controls described in the NZISM, any relevant legislation and regulation, MSD's Policies and Standards, and other relevant standards. It is based on a comprehensive evaluation or systems audit.

Word / Phrase	Definition
	Certification is evidence that due consideration has been paid to risk, information security, functionality, and business requirements, and is a fundamental part of systems governance and assurance.
Control	Measure or mechanism that is in place to manage and/or reduce the likelihood or consequence of the risk. Controls should have a Control Owner assigned to them.
Data Sovereignty	Data Sovereignty typically refers to the understanding that data is subject to the laws of the nation within which it is stored. Indigenous Data Sovereignty perceives data as subject to the laws of the nation from which it is collected. Māori Data Sovereignty recognises that Māori data should be subject to Māori governance. Māori data sovereignty supports tribal sovereignty and the realisation of Maori and Iwi aspirations.
DPMC (Department of the Prime Minister and Cabinet)	The DPMC's overall area of responsibility is in helping to provide, at an administrative level, the 'constitutional and institutional glue' that underlies our system of parliamentary democracy and serves the Executive, Governor-General, Prime Minister and Cabinet, through the provision of impartial advice and support.
Exceptional circumstances	Exceptional circumstances means circumstances that could not be reasonably foreseen that require supporting critical MSD functions and that would, if not performed, cause adverse impacts to MSD's operations. For example, for the purpose of business continuity.
MSD Staff	Includes employees, contractors, consultants, temporary staff, and other workers at MSD, including all personnel affiliated with third parties.
NZISM (New Zealand Information Security Manual)	Details processes and controls essential for the protection of all New Zealand Government information and systems. Controls and processes representing good practice are also provided to enhance the baseline controls. Baseline controls are minimum acceptable levels of controls and are often described as "systems hygiene".
People	Includes MSD Staff, clients, and partners.
PSR (Protective Security Requirements)	The PSR outlines the Government's expectations for managing personnel, physical and information security.
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.
Third parties	MSD forms working relationships with a variety of third parties to help New Zealanders be safe, strong, and independent. Third parties: (i) includes, but is not limited to, other government agencies or crown entitles, private entities or non-government organisations (NGOs) and charities, iwi, or community groups. (ii) do not include clients of MSD (in their personal capacity only) or the general public.

Word / Phrase	Definition
Risk	An uncertainty or event that may have an impact on MSD operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Work events	Work events means events that occur in connection with a person's employment such as attending conferences or delegations.

8 Related Policies, Standards and Guidelines

Policy / Standard / Guideline	Purpose	Link
Information Security Policy	This policy defines the principles, roles, and responsibilities which support MSD in upholding its Information Security responsibilities to the New Zealand Government and public. The principles found in this policy set the governing direction and intent for Information Security. Underpinning this policy are standards, patterns, processes, and guidance material which collectively operationalise the principles in this policy and align MSD 's Information culture and decision-making.	Objective EDRMS Link
Remote Access Standard	This Standard applies to all MSD users who undertake work for or on behalf of MSD (e.g., MSD Staff) and access MSD Systems remotely (i.e., not from an MSD office).	MSD Remote Access Standard.pdf

9 References

- Protective Security Requirements (PSR) Advisories
  - **"Working from overseas - security considerations for agencies" and "Questions for consideration"** (Report Date: 21 March 2023; Report No: DMS26-4-8413)
- DPMC Jurisdiction Assessment Framework, version 1.0, July 2017
  - The DPMC Jurisdiction Assessment Framework is due to be updated in 2023.
- GCIO Cloud Assessment Guidance and GCIO Cloud Assessment Tool
- New Zealand Information Security Manual (NZISM) - Version 3.6 (Last updated on September-2022) – Sections:
  - 22.1. Cloud Computing
  - 23.4. Data Protection in Public Cloud
- OHC-Memo-Offshore-Working (A15118195) presented to OHC on 8th June 2023.

Digital Information Standard

Approved by:	Fiona McElwee, Director Information Policy, Capability and Operations on 17/11/2025
Standard Owner:	Magnus O'Neill
Next Review Date:	November 2027
Review Committee	Policies and Standards Working Group

1 Purpose

This standard describes the Ministry of Social Development (the Ministry) expectations and requirements for creating information in digital format and for converting physical information to digital format. Digital format helps the Ministry to monitor and ensure the integrity, discoverability, accessibility, and confidentiality of information. It is also easier to manage digital information through its lifecycle in comparison to physical information. Creating and managing information in digital format therefore supports the Ministry to deliver its functions and services to clients as well as to meet obligations set by the Public Records Act 2005.

This standard supports and enables the principles in the Information Governance Policy that describe how the Ministry manages information assets in accordance with legislative obligations, how Information Asset Owners are responsible for ensuring the risks to their information assets are understood and managed, and that the quality and integrity of Ministry information assets is maintained.

2 Scope

This standard applies to all information created, collected, or obtained for Ministry business that 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.

3 Standard

3.1 Digital Information

3.1.1 All Ministry information ***must*** be created and managed in digital format so that its integrity, availability, and confidentiality is protected throughout its lifecycle. Digital approval methods ***should*** be used wherever possible, e.g., digital signature.

3.1.2 New business processes ***must*** only create or collect physical information for accessibility purposes with the intent to then digitise the physical information. Digital channels ***must*** also be available.

3.1.3 Information ***must*** be created or collected in a digital format that ensures it will remain manageable and accessible over time to enable future use.

3.2 Converting Physical Information to Digital Format

3.2.1 If information is provided to the Ministry in physical format, it ***must*** be converted to a digital format.[1]

3.2.2 Digitisation ***must*** only occur after all editing or annotation of the physical copy is finished.

3.2.3 The physical version ***must*** only serve an operational or transactional purpose. It ***must*** be disposed of as a duplicate as soon as the authoritative digital record is captured in a Ministry approved system.

3.2.4 The digital version of physical information ***must*** be considered the authoritative record, including where a document contains a signature.

3.2.5 Information Asset Owners ***must*** ensure any risks to their physical information assets are appropriately managed. Information Asset Owners ***must*** contact the Information, Privacy and Security Group (IPS) for advice where Ministry information is discovered that:

- is physical and has high business value, or
- is physical and at risk of information loss (e.g., is fire or flood damaged, or conversion to digital format is poor quality).

4 Standard Compliance

4.1 Exceptions

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

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

4.1.3 Compliance to this standard does not apply to the following categories of public records as they are excluded from the Chief Archivist's general approval to retain public records in digital form only:

- unique or rare information, information of importance to national or cultural identity or information of historical significance
- unique or rare information of cultural value to Māori (land and people) and their identity
- all information created prior to 1946
- public records that are the subject of a legal requirement to retain information that is in paper or any other non-electronic form, contained in certain enactments or provisions specified in Schedule 5 of the Contract and Commercial Law Act 2017.

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.

[1] Certain categories of public records are exempt from this requirement. See 4.1.3.

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
October 2025	Tallulah Willis	Minor changes made for clarity and to align with and support MSD's goal to work digitally. Changes are low risk and low impact.

6 Definitions

Word / Phrase	Definition
Approved repository	A repository approved by MSD that meets business, legislative and information requirements.
Authoritative record	A record that meets all the characteristics of a record (authentic, reliable, identifiable, retrievable, accessible, and useable) so decisions can be confidently made.
Digital Format	Digital format is information (structured or unstructured) that is accessible via a computer or other technology-based system or process.
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.

Physical Information	This includes, but is not limited to, paper files, film, tape, computer discs, CD's, microfilm and microfiche.
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.
Technological Obsolescence	Where technology or components of, are replaced by newer versions making either the hardware, software or physical carrier obsolete and therefore the information unreadable or accessible.

7 Related Standards

Standard	Purpose	Link
Information Classification	Information in digital format can have a classification label applied and be managed in accordance with the security requirements for that classification.	Information Classification
Information Retention and Disposal	Describes requirements for retaining information so it can be managed through its lifecycle and for disposing of information.	Information Retention and Disposal
Minimum Metadata Capture	Metadata must be captured for all digital information, and physical information tracked in a system, so it can be understood and managed.	Minimum Metadata Capture

8 References

Information Governance Policy

Information Classification Standard

Information Retention and Disposal Standard

Minimum Metadata Capture Standard

Public Records Act 2005

Archives New Zealand Information and Records management standard 2016

Archive New Zealand File format Migration

Subpart 3 of Part 4 of the Contract and Commercial Law Act 2017, especially sections 218, 221, 222 and 229.

Archives New Zealand Authority to retain public records in electronic form only

Archives New Zealand Destruction of source information