Information Governance Policy

Last Review Date:	October 2022
Next Review Date:	October 2024
Approved by:	Organisational Health Committee
Owner:	General Manager Information

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 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 legislative requirements defined in the Public Records Act 2005, Privacy Act 2020, the Protective Security Requirements (PSR) and the Official Information Act (1982). The Ministry's standards define the measures which set the baseline for how information assets are secured, stored, used, and managed using a risk-based approach.

2. All information assets held by the Ministry have responsible owners to ensure they are managed appropriately

An information asset has value to the Ministry from the point of creation or collection through to eventual disposal. Information asset owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored throughout the lifecycle. Any legal and regulatory requirements applicable to the collection, storage and use 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 integrity of Ministry information assets ensures people use authoritative information. The information collected, used, and shared by the Ministry is appropriate for the purpose 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 MSD to support Māori

The Ministry invests in trusted partnerships with Māori and ensures it embeds the needs of Māori in the ways it protects, stores, uses, and maintains Māori data and information. The Ministry recognises Māori data as taonga and manages it as such. In acknowledging its Te Tiriti o Waitangi responsibilities, the Ministry is committed to partnering with Māori in decisions made to govern Māori data and information assets.

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

Ministry staff are responsible for handling Ministry-held information and data appropriately. While Ministry technology and processes play a key role in providing a layer of protection over information, 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 IT security, 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, 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 it is managed effectively at the appropriate level and in a timely way • Reporting any IT security, information security or privacy incidents to their line manager
Information Asset Owners	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.
Information Stewards	Information Stewards are responsible for the quality, integrity, and responsible use of information assets, enabling the organisation to gain maximum value from the information. They are also responsible for 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 made aware of any risks or concerns surrounding the integrity or safety of information. At MSD, Information Stewards will typically be General Managers, Regional Directors and Directors.
Information Governance Committees	Information governance committees are responsible for overseeing and tracking the achievement of the Ministry's strategic objectives relating to information governance.

Person/Party	Responsibility
	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 MSD, the Information Governance Committees consist of the Leadership team (LT), Organisational Health Committee (OHC) and the Technical Design Committee (TDC).
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 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 MSD, the CSO is the DCE Organisational Assurance and Communication.
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 MSD, 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 MSD, the CPO is the GM Information.
Chief Analytics Officer	The Chief Analytics Officer (CAO) oversees the analytics function, including data analytics and data science. They set strategic priorities for this function and identify new opportunities for the Ministry based on data. The CAO is responsible for: • Managing the analytics needs across the organisation • The creation of data warehouses • Data governance and data management frameworks At MSD, the CAO is the GGM Insights.
Information Group	Information 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 and comply with information legislation and related regulations • Delivering a foundational capability - providing direction, guidance tools, training and support to ensure information capability improvements can be achieved
Insights	The Insights Group is responsible for: • 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.

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 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, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion
Information Governance	Information governance is the capabilities, processes, controls, oversight, and assurance relating to information security, privacy, sharing and management. Information governance requires the specification of decision rights and an accountability framework to ensure appropriate behaviour across the information lifecycle. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals.
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 MSD 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".
Privacy	Privacy relates to the rights you have to control your 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.