RBNZ information and data management

Policy statement | Te ito o te kaupapa-here

This policy sets out our principles for managing our information and data to meet legislative and government obligations, fulfil our purpose, contribute to our wānanga, and support the mahi we do on behalf of all New Zealanders.

It ensures our information and data are:

- open and readily available for public access unless protection is required
- protected according to type and classification
- well-managed through lifecycles and across platforms
- trusted and authoritative
- reusable throughout their lifecycle and changes in technology.

Application and definitions | Te Whakamahinga me te Tautuhi

This policy applies to all information and data held by Te Pūtea Matua.

Information[1] means any material that bears symbols including words and figures, images, or sounds, or material from which symbols, images, or sounds can be derived. It includes:

- labels, marking, or other writing that identifies or describes a thing of which it forms part, or to which it is attached
- books, maps, plans, graphs, and drawings
- photographs, film, or negatives
- information electronically recorded or stored.

Data[2] means the type of information that is collected to be categorised, analysed, and/or used to help decision-making. It can exist in various forms such as numbers or text recorded on paper, and as bits or bytes stored in electronic memory.

[1] This meaning is from the interpretation given in the Reserve Bank of New Zealand Act 2021.

[2] This meaning is from the definition provided by data.govt.nz, with form definitions from Webopedia.

Contents | Te kiko

1. Principles | Mātāpono

1. Collectively we are kaitiaki of our information and data, recognising these as valued core assets vital to our mahi.
2. We comply with all statutory and contractual legal obligations in managing our information and data.
3. We determine our compliance with discretionary requirements and standards in line with the nature and context of specific information or data, and its use or handling within Te Pūtea Matua.
4. We commit to the ethical, culturally-appropriate gathering and use of information and data from communities of distinct ethnic and cultural identity.
5. We only acquire, generate, and hold information and data for which we have a genuine business purpose.
6. We embrace an open information and data culture based on trust and respect, only restricting access where there is a legal, ethical, protective, or operational requirement to do so.
7. We make the right information or data available to the right person, at the right time, in the right format, via the right medium.

2. Strategy and investment

As our information and data are core assets, vital to our mahi, we will:

- have a vision for information and data management in alignment with our strategic direction and business objectives
- articulate and resource the strategy for achieving the vision
- prioritise the delivery of strategic initiatives based on business value and risk assessment.

3. Organising to manage information and data

To ensure we meet our information and data governance obligations, we will:

- maintain an information and data governance framework commensurate with RBNZ's size, with clear responsibilities and terms of reference
- provide support to people with information governance and management responsibilities through communication, documentation, and professional development
- record specific information and data management requirements in policies and standards.

4. Information and data lifecycles

To ensure our information and data is reusable, trusted, and authoritative throughout its lifecycle, we will:

- maintain standards for managing our information through all stages of its lifecycle
- set in place processes, systems and tools to assure the quality of:
  - data and information that is collected and generated
  - media, systems, and locations used for processing and storage
  - tools used for data transformation and analysis
  - archiving and disposal methodologies and tools
  - partners and suppliers who provide associated services.
- run an assurance programme which confirms the application of good practice.

5. Information, data, and systems security

To protect our physical and electronic information and data from unauthorised access, disclosure, misuse, or corruption we will:

- identify vulnerabilities and manage risks to our information and data at all stages of the lifecycle
- maintain and communicate information and data security, privacy, and disclosure policies
- apply approved RBNZ security classifications to information, data, and repositories as required, including labelling physical areas and tools
- control access to our information, data, and systems, including access to physical locations where these are stored where appropriate
- ensure security and privacy requirements are included by design in information and data management processes, tools and systems
- provide generic training in information security and privacy for all persons employed or engaged by RBNZ, to be completed annually
- provide role-specific training and support for people who have classified or other special information-handling responsibilities
- require all people employed or engaged by RBNZ to commit to our information security and privacy policies at on-boarding and annually.

5.1. Third party contractors

Where third party contactors will have access to our information, data, and the supporting technology we will:

- require suppliers, their staff, and their contactors who will have with access to our information, data, and systems to enter into appropriate confidentiality agreements before they commence work, to be updated annually
- require every individual with access to our information, data, and systems to commit to our information security, privacy, and handling policies before they commence work, and require annual re-commitment
- check periodically that suppliers, their staff, and their contractors are complying.

6. Handling and using internally

To maintain an open data culture and ensure we are getting maximum benefit from our information and data we will:

- use an agreed information architecture to organise our information and data
- manage access to information and data according to its type, purpose, use, classification, and endorsements

- respect intellectual property and ownership, including respecting Māori IP rights in our use of Māori imagery and Te Reo
- maintain and communicate policies for handling specific information types
- provide training in specific systems for end-users
- run a service desk to support users of information and information systems
- enable information use to be tracked or discovered
- use our intranet to publish information such as policies and operational documentation that affect all staff
- have a communication plan for all matters affecting information management stakeholders.

7. Sharing and disclosing externally

To support the Government's open data policy, and in response to requests for information and data, we will:

- publish information that can be shared publicly on our internet site
- respond to official information and privacy requests and parliamentary questions in the legally-prescribed manner
- comply with our policies and internal processes for responding to requests for information and data from other agencies or individuals
- use secure systems and tools for sharing classified information with approved agencies
- provide training for all staff to limit the risk of unintended disclosure.

8. Technology for information and data management

To ensure our information technology infrastructure is reliable, secure, and fit for purpose, we will:

- maintain an information technology infrastructure, designed in response to our business requirements, and with security and privacy at the forefront of any system procurement or design
- use only RBNZ-approved technology patterns, systems, and tools
- ensure interoperability with stakeholders such as Treasury, banks, non-bank deposit takers, and suppliers as required
- provide the technical capability to continue our operations and minimise disruptions from internal or external events
- protect our physical and virtual infrastructure from unauthorised access, use, or attack
- comply with information and data technology directions set by the Government.