



Information and records management standard

July 2016

A mandatory standard issued under Section 27 of the Public Records Act 2005 by
the Chief Archivist



New Zealand Government

Document details

Document Identifier: 16/S1

Version	Date	Description	Revision due
0.1	Mar 2016	Development Draft	
0.2	May 2016	Final draft. Updated with consultation feedback.	
1.0	Jul 2016	Final version for Chief Archivist's approval and issue.	

Acknowledgement

This standard is based on the State Records Authority of New South Wales' *Standard on records management* issued in 2015.

Contact for enquiries

Government Recordkeeping Directorate
Archives New Zealand
Phone: +64 4 499 5595
Email: rkadvice@dia.govt.nz

Licence



Crown copyright ©. This copyright work is licensed under the Creative Commons Attribution 3.0 New Zealand licence. In essence, you are free to copy, distribute and adapt the work, as long as you attribute the work to Archives New Zealand, Department of Internal Affairs and abide by the other licence terms. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/3.0/nz/>.

ISBN 978-0-478-43052-3

ISSN 1176-2713

CONTENTS

1	Introduction.....	4
1.1	Why we have an information and records standard	4
1.2	Mandate	5
1.3	The Treaty of Waitangi / Te Tiriti o Waitangi.....	5
1.4	Further information	5
2	Principles	6
	Principle 1: Organisations are responsible for managing information and records	6
	Principle 2: Information and records management supports business	8
	Principle 3: Information and records are well managed.....	10

1 Introduction

Information and records are key strategic assets at the core of public sector business and government accountability. They help organisations plan for and achieve valuable and relevant short-term and long-term outcomes that benefit business, government and the wider community.

Managing information and records appropriately is important because it:

- enables the public to hold the government accountable
- provides the foundation for sustainable and effective products and services
- supports decision making
- outlines responsibilities
- documents rights and entitlements
- drives collaboration and communication
- facilitates and enables creativity and growth
- preserves public knowledge for discovery and reuse
- makes up the corporate memory of an organisation.

Information and records should therefore be:

- trustworthy and managed accountably
- readily accessible, understandable and usable
- valued as critical to business operations
- part of an organisation's approach to risk management
- maintained to meet business, government and community purposes.

1.1 Why we have an information and records management standard

This standard establishes how to manage information and records efficiently and systematically. It sets out the minimum level of compliance that organisations must meet.

This standard is designed to support organisations to meet their obligations under the Public Records Act 2005 (the Act). A major focus of the standard is to support effective information and records practices in complex business and government environments.

Records are considered to be any information, regardless of form and format, from documents through to data. Records serve both as evidence of business activity and as information assets. A record includes its metadata, which is also managed as a record. Meeting the standard enables organisations to manage their information assets in a holistic, integrated manner. The standard should be read in conjunction with instructions, directions, and any other standards or guidance under the Act.

1.2 Mandate

This standard is issued by the Chief Archivist under section 27 of the Act. It is mandatory for the following organisations, which must manage their information and records to the standard:

- public offices, including state and integrated schools
- local authorities, including council-controlled organisations.

With the issuing of this standard, the following standards have been revoked as Archives New Zealand standards:

- Records Management Standard for the New Zealand Public Sector (2014)
- S4: Access Standard (2006)
- S5: Digital Recordkeeping Standard (2010)
- AS/NZS ISO 13028: 2012, Information and documentation – Implementation guidelines for digitization of records

1.3 The Treaty of Waitangi / Te Tiriti o Waitangi

The standard supports the rights of Māori, under the Treaty of Waitangi / Te Tiriti o Waitangi to access, use and reuse information and records that are taonga. Organisations should ensure that information and records about Māori are accessible.

1.4 Further information

To assist organisations in implementing this standard, Archives New Zealand has linked the minimum compliance requirements to key guidance. This linking, along with an explanation of each requirement, is available in the *Implementation* guide.

2 Principles

Principle 1: Organisations are responsible for managing information and records

To ensure information and records are able to support all business functions and operations, organisations must establish a governance framework. This framework will help an organisation to:

- develop strategies and policies to direct how information and records will be managed
- assign responsibilities and allocate resources
- establish provisions for information and records management in outsourcing and service delivery arrangements
- monitor information and records management activities, systems and processes.

Minimum compliance requirements	Examples of how an organisation can demonstrate compliance with the requirement
<p>1.1 Information and records management must be directed by strategy and policy, and reviewed and monitored regularly.</p>	<ul style="list-style-type: none"> • Ensure senior executives adopt an organisation-wide strategy on information and records management. • Ensure senior executives adopt an organisation-wide policy on information and records management. • Monitor how people in the organisation are applying strategies and policies.
<p>1.2 Information and records management must be the responsibility of senior management. Senior management must provide direction and support to meet business requirements as well as relevant laws and regulations.</p>	<ul style="list-style-type: none"> • Ensure the policy lists the senior executive team as responsible for managing information and records. • Ensure the policy reflects the legislative responsibilities of chief executives for example under the State Sector Act 1988 (section 32(1)), and the Local Government Act 2002 (section 42(2)).
<p>1.3 Responsibility for the oversight of information and records management must be allocated to a designated role (the Executive Sponsor).</p>	<ul style="list-style-type: none"> • Include the Executive Sponsor's responsibility in all strategy and policy on information and records management. • Include the Executive Sponsor's responsibility in their performance plan. • Advise Archives New Zealand of the organisation's Executive Sponsor.
<p>1.4 Organisations must have information and records management staff, or access to appropriate skills.</p>	<ul style="list-style-type: none"> • Assign responsibility for information and records management to appropriate staff, and record these responsibilities in all strategies and policies. • Note the skills and capabilities in relevant role descriptions. • Include responsibilities in performance plans and service agreements.

Minimum compliance requirements	Examples of how an organisation can demonstrate compliance with the requirement
<p>1.5 Business owners and business units must be responsible for ensuring that information and records management is integrated into business processes, systems and services.</p>	<ul style="list-style-type: none"> • Include and list all assigned responsibilities in the policy on information and records management. • Include and list all assigned responsibilities in performance plans. • Include in systems and processes details about responsibility for ensuring effective information and records management. • Document the responsibility of the business owner.
<p>1.6 Staff and contractors must understand the information and records management responsibilities of their role. They must understand relevant policies and procedures.</p>	<ul style="list-style-type: none"> • Note the skills, capabilities and responsibilities in the relevant role descriptions and performance plans. • Set out in all policies, business rules and procedures the requirements and responsibilities for all staff who create and manage information and records.
<p>1.7 Information and records management responsibilities must be identified and addressed in all outsourced and service contracts, instruments and arrangements.</p>	<ul style="list-style-type: none"> • Note all responsibilities in the strategy and policy on information and records management. • Specify and detail in outsourced and service contracts, instruments and arrangements all aspects of information and records management. • Assess portability and security of information and records in all outsourced and service contracts, instruments and arrangements.
<p>1.8 Information and records management must be monitored and reviewed to ensure that it is accurately performed and meets business needs.</p>	<ul style="list-style-type: none"> • Document monitoring activities, systems and processes; take corrective actions to address any problems. • Ensure reviews of all processes and systems happen regularly.

Principle 2: Information and records management supports business

Information and records management ensures the creation, usability, maintenance, and sustainability of the information and records needed for business operations. It also ensures business operations meet government and community expectations.

By appraising business activities, organisations define their key information requirements. Appraisal is used to design and embed information and records management into business processes and systems.

Taking a planned approach to information and records management means:

- considering all operating environments
- ensuring that all service and systems arrangements consider the creation and management of information and records needed to support business.

Minimum compliance requirements	Examples of how an organisation can demonstrate compliance with the requirement
<p>2.1 Information and records required to support and meet business needs must be identified.</p>	<ul style="list-style-type: none"> • Document policies, business rules and procedures on what information and records are required to meet and support business needs. • Current, comprehensive appraisal is documented. • Decisions are documented or reflected in specifications for systems and metadata schemas.
<p>2.2 High risk/high value areas of business, and the information and records needed to support them, must be identified and regularly reviewed.</p>	<ul style="list-style-type: none"> • Identify and document which parts of the organisation and which systems hold information and records that are high risk, high value, or both. • Identify, manage and mitigate all risks relating to the information and records. • Protect with business continuity strategies and plans all business areas and systems which manage information and records that are high risk, high value, or both.
<p>2.3 Information and records management must be design components of all systems and service environments where high risk/high value business is undertaken.</p>	<ul style="list-style-type: none"> • Assess information and records management in system acquisition, maintenance and decommissioning, and implement these practices where needed. • Ensure that systems specifications for business that is high risk, high value, or both, include information and records management requirements. • Ensure that systems specifications include minimum requirements for metadata needed to support information and records identification, usability, accessibility, and context. • Document and maintain systems design and configuration.

Minimum compliance requirements	Examples of how an organisation can demonstrate compliance with the requirement
<p>2.4 Information and records must be managed across all operating environments.</p>	<ul style="list-style-type: none"> • Identify and document where information and records are created and held, across all system environments and physical locations. • Document the process for managing information and records in diverse system environments.
<p>2.5 Information and records management must be designed to safeguard information and records with long-term value.</p>	<ul style="list-style-type: none"> • Document which systems hold information and records of long-term value or archival value, and where they are located. • Ensure that the decommissioning of systems follows the requirements for disposing of information and records.
<p>2.6 Information and records must be maintained through systems and service transitions by strategies and processes specifically designed to support business continuity and accountability.</p>	<ul style="list-style-type: none"> • Implement and review a migration strategy. • Migrate information, records and metadata from one system to another using a managed process that results in records that people can access easily and that have trustworthy information. • Ensure the portability of information and records is addressed in outsourced or service arrangements. • Maintain the systems documentation.

Principle 3: Information and records are well managed

Effective management underpins trustworthy and reliable information and records that are accessible, usable, shareable and maintained. This management extends to information and records in all:

- formats (and associated metadata)
- business environments
- types of systems
- locations.

Minimum compliance requirements	Examples of how an organisation can demonstrate compliance with the requirement
<p>3.1 Information and records must be routinely created and managed as part of normal business practice.</p>	<ul style="list-style-type: none"> • Ensure all policies, business rules and procedures accurately document staff requirements and responsibilities for creating, capturing and managing information and records of business processes. • Ensure assessments or audits demonstrate that business rules, procedures and systems are operating. • Identify, resolve and document any exceptions to normal business processes that affect information integrity, usability or accessibility.
<p>3.2 Information and records must be reliable and trustworthy.</p>	<ul style="list-style-type: none"> • Ensure appropriate minimum metadata is available so that the meaning and context are associated with the relevant information and records, and that it is correct. • Ensure assessments or audits can test management controls, including information integrity.
<p>3.3 Information and records must be identifiable, retrievable, accessible and usable for as long as they are required.</p>	<ul style="list-style-type: none"> • Ensure testing is able to verify that systems can locate and produce information and records that are viewable and understandable. • Ensure appropriate minimum metadata is in place so that information and records are identifiable, accessible and usable.
<p>3.4 Information and records must be protected from unauthorised or unlawful access, alteration, loss, deletion and/or destruction.</p>	<ul style="list-style-type: none"> • Ensure information security and protection mechanisms are in place. • Protect information and records wherever they are located, including in transit and outside the workplace. • Document and implement all permissions to access and use systems that manage information and records. • Ensure that assessments or audits can test that access controls are implemented and maintained.

Minimum compliance requirements	Examples of how an organisation can demonstrate compliance with the requirement
<p>3.5 Access to, use of and sharing of information and records must be managed appropriately in line with legal and business requirements.</p>	<ul style="list-style-type: none"> • Ensure policies, business rules and procedures identify how access, use and appropriate sharing of information and records are managed. • Ensure assessments or audits confirm that access is in line with the organisation's policies, business rules and procedures.
<p>3.6 Information and records must be kept for as long as needed for business, legal and accountability requirements.</p>	<ul style="list-style-type: none"> • Ensure policies, business rules and procedures identify how the disposal of information and records is managed. • Ensure information and records are sentenced (a decision is made about whether to keep, destroy or transfer them). • Dispose of information and records regularly, and in line with authorised disposal authorities. • Transfer information and records of archival value to Archives New Zealand, or to an approved repository, or to a local authority archive (when authorised).
<p>3.7 Information and records must be systematically disposed of when authorised and legally appropriate to do so.</p>	<ul style="list-style-type: none"> • Ensure policies, business rules and procedures set out how to manage the disposal of information and records (including metadata). • Ensure disposal is in line with authorised disposal authorities. • Document any disposal of information and records.