Implementation guide

Information and records management standard

September 2023

Te Rua Mahara o te Kāwanatanga
Archives New Zealand
Part of the Department of Internal Affairs
New Zealand Government

Document details

Document Identifier: 16/G8

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	Published	
2.0	Oct 2016	Updated with new guidance	
3.0	Dec 2016	Updated with new guidance	
4.0	May 2017	Updated with new guidance	
5.0	Aug 2017	Updated with new guidance	
6.0	Dec 2017	Updated with new guidance	
7.0	Aug 2018	Updated with new guidance	
8.0	Dec 2020	Updated Key guidance column including links. Reformatted to new template.	
9.0	Feb 2020	Updated key links and standards	
10.0	May 2022	Updated links and standards. Added new guidance.	
10.1	Nov 2022	Updated Information Asset Catalogue Template link	
11	Sep 2023	Updated with new guidance. Clarified meaning of ‘revoked’.	

Contact for enquiries

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

Licence

Implementing the *Information and records management standard*

We have written this guide to help your organisation understand and apply the requirements of the *Information and records management standard* (16/S1) (the standard). The standard was issued by the Chief Archivist on 22 July 2016.

The standard's purpose

The standard covers information and records in any format. It has been designed to support digital recordkeeping as the public sector continues its transition to digital business processes. The purpose of the standard is to ensure that business is supported by sound, integrated information and records management in complex business and information environments. This approach better reflects the way that most organisations now manage their information assets.

The earlier standards

This standard is the result of consolidating and streamlining the requirements from these 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*

The standards above have been revoked as standards issued by the Chief Archivist and incorporated into this standard.[1]

Further requirements for local authorities and approved repositories

Local authorities and approved repositories must follow:

- the *Protection and preservation of protected records: Instruction to local authorities (16/Sp3)*
- the *Maintenance of public archives: Instruction to approved repositories (16/Sp2)*.

[1] Notes: This does not mean revoked as an ISO standard or any other standard issued by another authority or legislation.

How to implement the standard

This document sets out three principles:

Principle 1: Organisations are responsible for managing their information and records
Principle 2: Information and records management supports business
Principle 3: Information and records are well managed

Under each principle are listed the minimum compliance requirements, an explanation for each requirement, and key guidance for implementing the requirements. This guidance will be regularly added to.

Public offices and local authorities should use our Information Management Maturity Assessment (21/G19) and user guide (21/G20) to assess the strengths and weaknesses of their information management programmes to determine where improvements are most needed.

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 your 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	Explanation	Key guidance for implementing this requirement
1.1 Information and records management must be directed by strategy and policy, and reviewed and monitored regularly.	Governance frameworks are critical to the achievement of effective information and records management. Your organisation must set high-level strategy and policy for managing its information and records. The Administrative Head of your organisation must adopt it. Your strategy and policy should include: • appointment of an Executive Sponsor to oversee information and records management – requirement 1.2 • clear requirements for the creation, capture and management of information and records – requirement 3.1 • setting an information security policy – requirement 3.4	16/F4 Effective information and records management 16/F6 Key obligations - *Public Records Act 2005* 16/F9 Information and records management strategy 16/F10 Information and records management policy 16/F21 Information and records management capability

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	• identifying and assigning responsibilities of senior management for information and records management – requirement 1.2 • identifying the need for information and records management staff or skills (do this through performance plans and/or service agreements) – requirement 1.4 • identifying business owners responsible for including information and records management in all systems and processes – requirement 1.5 • setting information and records management responsibilities for staff and contractors – requirement 1.6 • addressing information and records management in all service arrangements – requirement 1.7 • implementing an information security policy and appropriate security mechanisms – requirement 3.4 • implementing policies (and business rules and procedures) to ensure that information and records are kept for as long as they are required and to identify how their disposal is managed – requirement 3.6 • implementing policies to identify how to manage the disposal of information and records – requirement 3.7.	Association of Local Government Information Management - Information Management Toolkit
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.	Ultimate responsibility for information and records management lies with the administrative head and senior management. They must provide direction and support and ensure information and records management meets business requirements, the law and regulations. Responsibility for information and records management is cascaded down throughout the organisation, through various levels of management. Responsibilities are identified and assigned in strategy and policy. This requirement mirrors legislative obligations for example in the *Public Service Act 2020* (s. 52) and the Local Government Act 2002 (s.42(2)) and reinforces the need for the Administrative Head and senior management to provide high-level direction and support, including ensuring adequate resourcing for information and records management.	16/F6 Key obligations - *Public Records Act 2005* AS/NZS ISO 30302:2016 Information and documentation – Management systems for recordkeeping – Guidelines for implementation Association of Local Government Information Management - Information Management Toolkit

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
1.3 Responsibility for the oversight of information and records management must be allocated to a designated role (the Executive Sponsor).	This requirement clarifies what was implicit in the previous standards. The **Executive Sponsor** oversees information and records management. They must be a senior manager with organisation-wide influence and appropriate strategic and managerial skills. Their role is to: • provide oversight of information and records management within the organisation, including monitoring of information and records management to ensure that this meets the needs of the organisation • ensure responses to monitoring/reporting requests from us. Include establishing this role in your policies and strategies for information and records management. The Executive Sponsor's role should be incorporated into their performance plan. Your organisation must advise us of your Executive Sponsor, when they are appointed and when the role changes hands.	16/F7 Monitoring 16/F11 Executive Sponsor - Role and Responsibilities 16/F21 Information and records management capability AS/NZS ISO 30302:2016 Information and documentation – Management systems for recordkeeping – Guidelines for implementations Association of Local Government Information Management - Information Management Toolkit
1.4 Organisations must have information and records management staff, or access to appropriate skills.	Your organisation must have staff with information and records management skills or be able to access this expertise. Each organisation's information and records management strategy will likely need a range of different levels of responsibility and skills. Reflect this in job descriptions. You must be able to access information and records management skills through recruitment, service providers, and by networking with other organisations. You must identify and assign responsibilities through strategy and policy, performance plans and/or service agreements.	16/G5 Providers of education and training in information and records management AS/NZS ISO 30302:2016 Information and documentation – Management systems for recordkeeping – Guidelines for implementations
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.	This **requirement** clarifies what was implicit in the previous standards. You must identify business and system owners who are responsible for ensuring information and records management is included in all systems and processes used. Those owners must be aware that information and records management requirements are needed when your organisation moves to a new service environment, develops new business processes, systems, or services, or changes existing business processes, systems, or services.	16/G2 Integrated information and records systems, processes and practices 20/G18 Microsoft 365 23/G23 Managing websites as records 23/F31 Web archiving 16/F9 Information and records management strategy

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	These responsibilities must be identified and assigned in policies and within performance plans. Business owners must demonstrate that they have considered information and records management requirements and assessed risks as part of any migration, development or improvement of systems or processes. This requirement places responsibilities more broadly within your organisation. It reflects the need for business managers to have a detailed understanding of the information and records produced by and necessary to perform their work, and their role in ensuring its management. Cascading responsibility to different business areas of your organisation enables business unit staff and information and records staff work together to ensure that information and records management is integrated into all business processes, systems, and services.	17/F22 Information assets - Overview 17/F23 Information assets - Identification 23/F36 Information assets - Management ict.govt.nz - Information Asset Catalogue Template ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles AS/NZS ISO 30302:2016 Information and documentation – Management systems for recordkeeping – Guidelines for implementations
1.6 Staff and contractors must understand the information and records management responsibilities of their role. They must understand relevant policies and procedures.	All staff of your organisation, including contractors, must understand their information and records management responsibilities. Policies, business rules and procedures must include clear requirements for staff when creating and managing information and records. External service providers may be contracted by your organisation to perform specified tasks. Information and records that are produced and managed in their performance of the contracted service(s) need to be covered by your organisation's policies and procedures. And contractors must know their information and records management responsibilities and the relevant policies and procedures. Information and records management responsibilities must be identified and assigned in policies. Skills, capabilities, and responsibilities must be assigned in role descriptions and performance plans.	16/G3 Outsourcing business 16/F6 Key obligations - Public Records Act 2005 16/F9 Information and records management strategy
1.7 Information and records management responsibilities must be identified and addressed in all outsourced and service contracts, instruments and arrangements.	This **requirement** clarifies what was implicit in the previous standards. Your organisation must ensure that information and records management is addressed in all service contracts, instruments, and arrangements. Your organisation's strategy and policy must include responsibilities to ensure that information and records requirements are identified and addressed. You must	16/G3 Outsourcing business 18/G15 Cloud services 16/F9 Information and records management strategy

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	undertake risk assessments and address information and records management requirements in contracts, instruments, and arrangements that your organisation agrees to. Service contracts, instruments and arrangements may include: • functions, activities, or services being outsourced to an external provider • functions, activities, or services being moved to cloud services or other service providers (internal or external to the New Zealand public sector). You must ensure that the portability of your organisation's information and records and associated metadata is assessed and appropriately addressed in any outsourced and service contracts, instruments, and arrangements.	16/F10 Information and records management policy data.govt.nz - New Zealand Data and Information Management Principles digital.govt.nz - Cloud digital.govt.nz - Security digital.govt.nz - Privacy New Zealand Government Procurement
1.8 Information and records management must be monitored and reviewed to ensure that it is accurately performed and meets business needs.	Your organisation must regularly monitor its information and records management activities, systems, and processes to ensure they are meeting its needs and conforming to any legislative requirements. Any issues identified though this monitoring must be addressed in a corrective action plan. You must monitor activities such as process and system audits of systems that are high-risk, high-value, or both. Any system of assurance for information and records management should be integrated into your wider organisational assurance processes. Your Executive Sponsor has responsibility for overseeing this monitoring.	16/F7 Monitoring 16/F11 Executive Sponsor - Role and responsibilities 16/F21 Information and records management capability AS/NZS ISO 9001:2016 Quality management systems – Requirements AS/NZS ISO 30302:2016 Information and documentation – Management systems for recordkeeping – Guidelines for implementations AS/NZS ISO 19011:2019 Guidelines for auditing management systems

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 your organisation's business operations. It also ensures these operations meet government and community expectations.

By appraising your organisation's business activities, you can define its key information and records requirements. Appraisal is an analysis process that can be used to plan, 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	Explanation	Key guidance for implementing this requirement
2.1 Information and records required to support and meet business needs must be identified.	This requirement provides the foundation for managing information and records in all environments. By analysing your organisation's functions, activities, and risks, you can identify what information and records it needs to support business. This analysis can also identify other requirements, including Treaty of Waitangi / Te Tiriti o Waitangi obligations, and government and community expectations. This analysis work provides the foundation for understanding what information and records to keep. It identifies what systems and business processes are high-risk and/or high-value for your organisation, and the information and records required to support these. You should incorporate this analysis into comprehensive and authorised disposal authorities for your organisation's information and records. Decisions about what information and records are required should be documented in your organisation's business rules, policies, and procedures. These decisions must also be reflected in specifications for systems and metadata schema.	16/G9 Disposal - Authorisation 16/F2 High-value and high-risk information and records 16/F10 Information and records management policy 16/F14 Appraisal of information and records 17/F22 Information assets - Overview 17/F23 Information assets - Identification 23/F36 Information assets - Management Te Titiri o Waitangi settlements and government records ict.govt.nz - Information Asset Catalogue Template ISO 15489-1:2016 Information and documentation – Records

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		Management Part 1: Concepts and principles, section 7 Association of Local Government Information Management - Information Management Toolkit
2.2 High-risk/high-value areas of business, and the information and records needed to support them, must be identified and regularly reviewed.	Your organisation must identify the areas of high risk, high value, or both of its business. This allows you to better prioritise how to manage, maintain and protect the information and records they need. You must identify the likely or potential risks to information and records and manage or mitigate them. This includes protecting the systems that manage information and records that are high-risk, high-value, or both, from loss and damage. You should set up appropriate security measures and business continuity strategies and plans. By identifying high-risk and high-value information and records at creation, your organisation can better manage and use these core assets.	16/F2 High-value and high-risk information and records 17/F22 Information assets - Overview 17/F23 Information assets - Identification 23/F36 Information assets - Management ict.govt.nz - Information Asset Catalogue Template data.govt.nz - New Zealand Data and Information Management Principles digital.govt.nz - Security digital.govt.nz - Privacy SA/SNZ HB 436:2013 Risk management guidelines – Companion to AS/NZS ISO 31000:2009 AS/NZS 5050:2010 Business continuity: managing disruption-related risk ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		SA/SNZ TR 18128:2015 Information and documentation – Risk assessment for records processes and systems Association of Local Government Information Management - Information Management Toolkit
2.3 Information and records management must be design components of all systems and service environments where high-risk/high-value business is undertaken.	This **requirement** clarifies what was implicit in the previous standards. In complex business and systems environments, it is important to design information and records management from the start. This is particularly important where the business involved is high-risk, high-value, or both. Include information and records management requirements when you design or update systems and service environments which manage high-risk and/or high-value information and records. This will enable you to manage and use the information and records. Your organisation must also consider at the start how to make system maintenance, migrations and decommissioning easier. In taking a "by design approach", you must ensure that systems specifications include: • requirements for managing information and records that are high-risk, high-value, or both • requirements for minimum metadata needed to support information and records identification, usability, accessibility and context • documentation about systems design, configuration and any changes made over time. Migrating and decommissioning systems can be expensive and time-consuming. Your organisation may hold insufficient documentation about: • the information and records held in the system(s) • the configuration of the system(s) • the disposal requirements for information and records held in the system(s).	17/Sp7 Authority to retain public records in electronic form only 16/G2 Integrated information and records systems, processes and practices 16/G7 Minimum requirements for metadata 17/G13 Destruction of source information after digitisation 16/F4 Effective information and records management 16/F8 Metadata for information and records 23/G23 Managing websites as records 23/F31 Web archiving Taonga Tuku Iho AS/NZS 5478:2015 Recordkeeping metadata property reference set AS/NZS ISO 13028: 2012 Information and documentation – Implementation guidelines for digitization of records, section 6.2 ISO 15489-1:2016 Information and documentation – Records

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		Management Part 1: Concepts and principles
2.4 Information and records must be managed across all operating environments.	Physical information and records are only part of your organisation's "operating environment" and this requirement widens the Standard to better cover digital information and records. If you know what information and records assets your organisation has and where they are located and managed, then you can better control them. By maintaining visibility of information and records, no matter what system is used or where the information and records are stored, your organisation can better protect these assets. Information and records assets can be held in diverse systems environments, including third-party systems in the cloud, by service providers, and in a range of physical locations. By identifying where your information and records are held, you can better manage them across diverse systems, storage environments or physical locations, and control their appropriate access.	17/Sp7 Authority to retain public records in electronic form only 17/G13 Destruction of source information after digitisation 17/G14 Managing information and records during administrative change 18/G15 Cloud services 20/G17 Best practice guidance on digital storage and preservation 16/F3 Text messages 16/F13 Storage of physical records 17/F22 Information assets - Overview 17/F23 Information assets - Identification 23/F36 Information assets - Management 23/G23 Managing websites as records 23/F31 Web archiving Audiovisual storage Care of motion picture film data.govt.nz - New Zealand Data and Information Management Principles digital.govt.nz - Security digital.govt.nz - Privacy

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		AS/NZS ISO 13028: 2012 Information and documentation – Implementation guidelines for digitization of records, section 6.2 and 6.4 Association of Local Government Information management - Information Management Toolkit
2.5 Information and records management must be designed to safeguard information and records with long-term value.	This requirement ensures that your organisation identifies which systems and service environments hold information and records with long-term business value. This requirement builds on *Requirements 2.1 and 2.2.* Once you know what information and records your organisation needs long-term and where they are kept, you can safeguard and manage them. Information and records required for the long-term will outlive both the systems in which they are managed, as well as any outsourcing arrangements or contracts with service providers. You must ensure you plan and manage the protection of long-term information and records during any system or service changes. Your organisation must protect its long-term information and records during changes in administration and through changes in the machinery of government. This includes where information and records may be transferred between organisations with functions. To assist with identifying long-term information and records, you should refer to your organisation's authorised disposal authorities.	16/G2 Integrated information and records systems, processes and practices 16/G9 Disposal – Authorisation 16/F14 Appraisal digital.govt.nz - Security digital.govt.nz - Privacy Association of Local Government Information Management - Information Management Toolkit
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.	This requirement makes the standard's focus more explicit to include both physical and digital information and records. Your organisation must ensure that information and records are managed appropriately through system migrations and service transitions, including upgrades of systems and services offered in cloud environments.	17/Sp7 Authority to retain public records in electronic form only 16/G2 Integrated information and records systems, processes and practices 16/G3 Outsourcing business

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	You must have documented migration strategies, and appropriate planning and testing processes. These must ensure that information and records are not "left behind" or disposed of unlawfully. You must use a managed process to migrate information and records and associated metadata from one system to another. The process must be managed to deliver information and records that are accessible, reliable and trustworthy. Maintaining appropriate system documentation will help to make migration strategies successful. You must use migration and decommissioning processes that ensure that information and records are kept for as long as needed for business, legal requirements (including in line with authorised disposal authorities), and government, and community expectations. This requirement builds on r*equirements 2.2* and *2.5*. These require that information and records that are high-risk, high-value, and/or long-term value, are supported and migrated appropriately. The portability of information and records and associated metadata must be assessed in any outsourced or service arrangements that your organisation has. Such arrangements must include provisions for transferring the information and records back to your organisation.	17/G14 Managing information and records during administrative change 17/G13 Destruction of source information after digitisation 18/G15 Cloud services 16/F15 Disposal of Information and records digital.govt.nz - Cloud AS/NZS ISO 13028:2012 Information and documentation – Implementation guidelines for digitization of records

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	Explanation	Key guidance for implementing this requirement
3.1 Information and records must be routinely created and managed as part of normal business practice.	Policies, business rules and procedures must inform staff in your organisation their responsibilities for creating, capturing and managing information and records. Your organisation must regularly monitor and assess or audit its information and records management practices to demonstrate that these business rules, procedures and systems are operating routinely. You must identify, resolve and document any exceptions that affect the creation, integrity, accessibility and usability of your organisation's information and records. Your organisation's staff and contractors must conform to these policies, business rules and procedures, to ensure information and records are routinely created and managed. The Executive Sponsor is responsible for overseeing this monitoring. This requirement builds on the earlier principles in the Standard.	16/G2 Integrated information and records systems, processes and practices 16/F7 Monitoring 16/F10 Information and records management policy ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles Association of Local Government Information Management - Information Management Toolkit
3.2 Information and records must be reliable and trustworthy.	Your organisation's information and records must have enough metadata to ensure they are reliable and trustworthy. Information and records must be accurate, authentic, and reliable as evidence of your organisation's transactions, decisions and actions. This requirement ensures that information	16/G7 Minimum requirements for metadata 16/F7 Monitoring 16/F8 Metadata for information and records 17/F25 Checksums - Overview

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	and records have appropriate minimum metadata to provide meaning and context (including te reo Māori terms), and that this metadata remains associated or linked. You must undertake regular assessments or audits to demonstrate that your management controls of business rules, procedures and systems are operating correctly. This provides assurance of the integrity of the information and records created and managed by your organisation. This requirement builds on the earlier principles in the standard.	AS/NZS 5478:2015 Recordkeeping metadata property reference set ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and Principles ISO 23081-1:2017 Metadata for records - Principles AS/NZS ISO 23081.2:2007 Metadata for records – Conceptual and implementation issues AS/NZS ISO 23081.3:2012 Managing metadata for records – Self assessment method Association of Local Government Information Management - Information Management Toolkit
3.3 Information and records must be identifiable, retrievable, accessible and usable for as long as they are required.	Your organisation's information and records must be identifiable, retrievable from storage (physical or digital), and accessible, usable and reusable for as long as required. To maintain the accessibility and usability of physical information and records, you must store them in appropriate storage areas and conditions. To maintain the accessibility and usability of digital information and records, you must ensure they are regularly migrated or moved from one system or platform to another. You must associate or link appropriate minimum metadata (including te reo Māori terms) to information and records to ensure they can be identified, retrieved and shared. Your organisation must regularly test all systems holding information and records. You must also perform assessments or audits to demonstrate that these systems can locate and produce information and records that people can read and understand. This requirement builds on the earlier principles in the standard.	16/Sp2 Maintenance of public archives (Instruction to approved repositories for physical (non-digital) archives 16/G7 Minimum requirements for metadata 20/G17 Best practice guidance on digital storage and preservation 16/F8 Metadata for information and records 16/F12 Public access to information and records 16/F13 Storage of physical records Audiovisual storage Care of motion picture film

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		Data.govt - Open data Digital.govt - Security Digital.govt - Privacy ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles Association of Local Government Information Management - Information Management Toolkit
3.4 Information and records must be protected from unauthorised or unlawful access, alteration, loss, deletion and/or destruction.	Your organisation must protect its information and records. You must implement an information security policy and appropriate security mechanisms. The policy must cover information and records held physically or digitally, or both. Security measures must include: • access and use permissions in systems holding information and records • processes to protect information and records no matter where they are located, including in transit and outside the workplace • secure physical storage facilities. Undertaking regular assessments or audits will help you verify that access controls have been implemented appropriately and are working.	16/Sp2 Maintenance of public archives (Instruction to approved repositories for physical (non-digital) archives 16/Sp3 Protection and preservation of protected records (Instruction to local authorities) 16/G6 Access decisions 16/F12 Public access to information and records 16/F13 Storage of physical records Digital.govt - Security Digital.govt - Privacy Ombudsman - Official information Guides

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		ISO 15489-1:2016 Information and documentation – Records Management Part 1: Concepts and principles Association of Local Government Information Management - Information Management Toolkit
3.5 Access to, use of and sharing of information and records must be managed appropriately in line with legal and business requirements.	This requirement builds on the requirements in Part 3 of the *Public Records Act 2005.* Your organisation must ensure that access to, use and sharing of information and records are in line with legal requirements including: • the *Official Information Act 1982* • the *Local Government Official Information and Meetings Act 1987* • the *Privacy Act 2020* • the *Health Information Privacy Code 1994* • organisational policies, business rules and procedures. Undertaking regular assessments or audits of systems holding information and records will help an organisation verify that access to, use and sharing of these information and records is managed in line with business requirements, legal obligations and the Government ICT Strategy or Action Plan (where appropriate).	16/F7 Monitoring 16/F12 Public access to information and records 21/F26 How to develop an OIA information search policy Digital.govt - Security Digital.govt - Privacy Ombudsman - Official information Guides Association of Local Government Information Management - Information Management Toolkit
3.6 Information and records must be kept for as long as needed for business, legal and accountability requirements.	Your organisation must implement policies, business rules and procedures to ensure that information and records are kept for as long as required, and to identify how their disposal or final fate is managed. These policies, business rules and procedures must be in accordance with the requirements of the *Public Records Act 2005* (the Act) and authorised disposal authorities. Your physical and digital information and records must be sentenced and disposed of in line with the instructions set out in disposal authorities authorised under the provisions of section 20 of the Act. This includes information and records located in business systems, in outsourced or service arrangements, or in offsite storage.	16/Sp4 List of protected records for local authorities 16/Sp5 GDA6: Common corporate service public records 16/Sp6 GDA7: Facilitative, transitory and short-term value records 17/Sp7 Authority to retain public records in electronic form only 16/G4 Explanatory notes for the List of protected records for local authorities

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
	Information and records of permanent value that are identified as public or local authority archives must be transferred to us, an approved repository or a local authority archive, when authorised and no longer needed for business purposes.	16/G10 Disposal - Sentencing 17/G13 Destruction of source information after digitisation 16/F1 Methods of destruction 16/F10 Information and records management policy 16/F15 Disposal of information and records 16/F16 General disposal authorities 16/G11 - Disposal – Transfer File format migration Association of Local Government Information Management - Information Management Toolkit
3.7 Information and records must be systematically disposed of when authorised and legally appropriate to do so.	This requirement builds on the earlier principles in the Standard. Your organisation must implement policies, business rules and procedures that identify how the disposal or final fate of information and records is managed. This includes: • assigning responsibility for sentencing and disposal of information and records (sentencing is the action of using a disposal authority to decide whether to keep, destroy or transfer information and records) • applying disposal authorisation processes • implementing disposal actions • deleting metadata • decommissioning systems • documenting the disposal of information and records. You must be able to account for the disposal of your information and records in business systems, outsourced arrangements, and offsite storage. This includes maintaining evidence that the disposal of information and records is permitted and authorised under disposal authorities' and legal obligations, including the *Public Records Act 2005*.	17/Sp7 Authority to retain public records in electronic form only 16/G9 Disposal - Authorisation 16/G10 Disposal - Sentencing 17/G13 Destruction of source information after digitisation 17/G14 Managing information and records during administrative change 16/F1 Methods of Destruction 16/F10 Information and records management policy 16/F15 Disposal of Information and records 16/G11 Disposal – Transfer

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
		23/F31 Web archiving Digital.govt -Security Digital.govt - Privacy Association of Local Government Information Management - Information Management Toolkit