Standard on records management

Introduction

Records, information and data are at the core of government business and are core assets.

Good recordkeeping is an important foundation for understanding government decisions and policies and creating trust in government.

In NSW public offices, records, information and data help organisations plan for and achieve short and long term outcomes that are relevant and valuable to the community, business and government. Records, information and data:

- drive collaboration, innovation and communications
- support evidence-based decision-making and policy development
- outline responsibilities
- mitigate business risk
- provide stakeholders with transparency around and accountability for government operations
- provide the foundation for sustainable and effective products and services
- document and support rights and entitlements
- preserve public knowledge for reference and reuse
- make up the corporate memory of an organisation.

To support these benefits, records, information and data need to be:

- trustworthy and managed accountably
- readily accessible, understandable and useable
- valued as critical to business operations
- governed by appropriate risk management approaches
- maintained securely to meet business, government and community purposes.

To achieve these outcomes, records, information and data must be supported by effective records and information management.

Section 12 of the State Records Act requires each public office to 'make and keep full and accurate records of the activities of the office' and 'establish and maintain a records management program for the public office'. Section 21 of the Act prohibits the abandonment, disposal, transfer, damage, or neglect of State records.

To assist public offices to understand and implement these obligations, State Records NSW has issued standards on records management since 1999, most recently in 2018. Following consultation with public offices, this revised version of the standard has been prepared for formal consultation in line with section 13 of the State Records Act.

1.1 Purpose

The purpose of this standard is to establish minimum requirements for effective records and information management. It is designed to assist public offices discharge their obligations under Part 2 'Records management responsibilities' and Part 3 'Protection of State records' of the *State Records Act 1998*, as well as incorporate records management requirements into new technologies and service delivery platforms.

1.2 Authority of this standard

This standard is issued under section 13(1) of the State Records Act which enables State Records NSW to 'approve standards and codes of best practice for records management by public offices'.

1.3 Who should use this standard

This standard applies to all public offices defined in section 3 of the State Records Act, to which Part 2 of the Act applies.

The standard applies to records created and maintained by contractors and service providers on behalf of public offices in the course of outsourced government business.

1.4 Scope of this standard

This standard covers records, information and data in all formats, including both digital and physical records.

Underpinning this standard is the need to ensure that business is supported by sound records and information management practices. Importantly, the standard has been framed and targeted to support good information practices in complex business and information environments.

This standard establishes requirements for the holistic management of records, information and data. Taking this approach better reflects the way in which most organisations now manage their information assets in an integrated manner.

This standard is not intended to replace data management practices but recognises the need for records and information management professionals to work closely with data custodians and/or managers. For data management policy and advice, see the NSW Government Data Strategy at https://data.nsw.gov.au/nsw-government-data-strategy .

To assist NSW public offices implement this standard, State Records NSW has mapped the requirements of the standard to the guidance and training available from State Records NSW. The mapping is available at https://staterecords.nsw.gov.au/guidance-and-resources/standard-records-management . Public offices should consult the *Standard on the physical storage of State records* for requirements for the storage of non-digital records and counter disaster requirements applicable to non-digital records.

1.5 Benefits of using this standard

Applying this standard will assist public offices to:

- create trustworthy, useful and accountable records, information and data in evolving business environments
- ensure that meaningful, accurate, reliable and useable records, information and data are available whenever required for government business needs
- sustain and secure the records, information and data needed to support short and long term business outcomes
- enable the reliable sharing of relevant records, information and data
- automate governance, sharing and continuity processes
- minimise records, information and data volumes, preventing unnecessary digital and physical storage and management costs
- proactively protect and manage the records, information and data that provide ongoing value to government business and to the community of NSW.

1.6 Structure

This standard sets out three principles for effective records and information management. Under each principle there is a brief explanation of the principle and a set of minimum compliance requirements.

1.7 Definitions

For the purposes of this standard, the following definitions apply. Terms that have not been referenced are taken from State Records NSW sources. All other sources are provided in brackets after the definition.

Recordkeeping

The process of making accurate and reliable records and capturing them into the official recordkeeping systems of the organisation.

Records management

Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition [disposal] of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records (*AS ISO 15489.1: 2017* – clause 3.15).

1.8 Further information

For more information on this standard, please contact State Records NSW.

Principles

Principle 1: Organisations take responsibility for records and information management

To ensure records and information are able to support all corporate business operations, organisations should establish governance frameworks. These include:

- policy directing how records, information and data shall be managed
- assigning responsibilities
- establishing provisions for records, information and data in outsourcing and service delivery arrangements
- monitoring records and information management activities, systems and processes.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
1.1 Corporate records and information management is directed by policy and strategy.	• Corporate policy on RM/IM has been endorsed at Senior Executive level. • Corporate policy on RM/IM has been communicated and made available to all staff and contractors. • Corporate strategy on RM/IM, aligned to the organisation's strategic direction, has been endorsed at Senior Executive level.
1.2 Records and information management is the responsibility of senior management who provide direction and support for records and information management in accordance with business requirements and relevant laws and regulations.	• Responsibility is assigned in corporate policy on RM/IM. • Policy reflects chief executive's responsibility to ensure compliance with section 10 of the State Records Act. • Delegations Manual is updated to include records and information management responsibilities and referenced in policy. • Information Governance group is established to oversee all aspects of records and information management.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
1.3 Corporate responsibility for the oversight of records and information management is delegated to a designated individual (senior responsible officer).	• Responsibility is assigned in corporate policy on RM/IM. • Delegations Manual is updated to include records and information management responsibilities and referenced in policy. • Responsibility is assigned in individual performance plans. • State Records NSW has been advised of the organisation's senior responsible officer.
1.4 Organisations have skilled records and information management staff or access to appropriate skills.	• Responsibility is assigned in corporate policy on RM/IM. • Skills and capabilities are reflected in relevant role descriptions. • Responsibility is assigned in performance plans and/or service agreements. • Organisation has assessed its records and information management capability and capacity against its business needs.
1.5 Responsibility for ensuring that records and information management is integrated into work processes, systems, and services is allocated to business owners and business units.	• Responsibility is assigned in corporate policy on RM/IM. • Responsibility is assigned in performance plans and/or service agreements. • Documentation identifies owners of systems. • Responsibility for ensuring the inclusion of records and information management in systems and processes is assigned to owners of systems.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
1.6 Staff and contractors understand the records and information management responsibilities of their role, the need to make and keep records, and are familiar with the relevant policies and procedures.	• Responsibility is assigned in corporate policy on RM/IM. • Skills, capabilities and responsibilities are reflected in relevant role descriptions and/or performance plans. • Policy, business rules or procedures articulate/document staff requirements and responsibilities for the creation and management of records. • Responsibilities are included in staff induction, awareness programs and ongoing corporate training.
1.7 Records and information management responsibilities are identified and addressed in all outsourced, cloud and similar service arrangements.	• Responsibility is assigned in corporate policy on RM/IM. • Records and information management is assessed in outsourced and service arrangements, and included in contracts and instruments where required. • Responsibilities are identified and monitored in outsourced, cloud and similar service arrangements. • Portability of records and information is assessed in outsourced, cloud and similar service arrangements.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
1.8 Records and information management is monitored and reviewed to ensure that it is performed, accountable and meets business needs.	• Monitoring of recordkeeping performance, systems and processes, and corrective actions undertaken to address issues. Monitoring activities are documented. • Records management and recordkeeping are evaluated as part of internal or external audits. • Performance and compliance of the organisation's records management are assessed using State Records NSW's Records Management Assessment Tool (RMAT). • Organisation has a structured approach to addressing non-compliance issues and ensuring continuous improvement of records and information management. • Reports on monitoring of the organisation's records management are prepared for the Audit and Risk Committee.

Principle 2: Records and information management support business

The core role of records and information management is to ensure the creation, maintenance, useability and sustainability of the records, information and data needed for short and long term business operations.

By undertaking an assessment of records and information needs, public offices can define their key business information. Public offices should use this assessment to identify high risk and/or high value records and design records and information management into processes and systems. This will ensure that records, information and data:

- support business operations and accountability requirements
- are protected and suitably resourced, and
- are sustained for the short and long term.

Taking a planned approach to records and information management means all operating environments are considered. It also means that the creation and management of records, information and data needed to support business are considered in all system and service arrangements.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
2.1 Records, information and data required to meet short and long term needs of the business are identified.	• Documented decisions, policy, business rules or procedures on what records information and data are required to meet or support business and identified recordkeeping requirements, including accountability and community expectations. • Current, comprehensive and authorised records retention and disposal authorities are in place. • Decisions are documented or reflected in specifications for systems and metadata schema.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
2.2 High risk and/or high value areas of business and the systems, records and information needed to support these business areas are identified.	• High risk and/or high value records, information, and data are included in the organisation’s list of key information assets. • Systems holding high risk and/or high value records, information and data are identified and documented. • Information risks are identified, managed or mitigated, and documented in an Information Asset Register. • High risk and/or high value records, information and data are protected by business continuity strategies and plans. • Documented policy, business rules and procedures for high risk and/or high value business processes include responsibilities for the creation and management of records, information and data.
2.3 Records and information management is a designed component of all systems and service environments where high risk and/or high value business is undertaken.	• Evidence that records and information management is assessed in system acquisition, system maintenance and decommissioning, and implemented where required. • Systems specifications for high risk and/or high value business include records and information management requirements. • Systems specifications include requirements for metadata needed to support records identification, useability, accessibility, and context. • Documentation of systems design and configuration maintained.
2.4 Records, information and data are managed across all operating environments.	• Information Asset Register identifies and documents where records, information and data are held across diverse system environments or physical locations. • Business rules and procedures are in place to manage records, information and data in diverse and evolving system environments or physical locations.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
2.5 Records and information management is designed to safeguard records, information and data, including records with long term retention.	• Systems holding records of identified or potential permanent or long term retention are identified and documented. • Locations of records identified for potential permanent or long term retention are documented. • Information Asset Register identifies and documents risks or barriers to accessibility to digital records and information, and informs migration strategies. • Information security and protection mechanisms are built into systems and processes to mitigate cyber security incidents and protect sensitive or confidential records, information and data. • Regular testing of information security and protection mechanisms. • Records, information and data are kept for as long as they are needed for business, legal requirements (including in accordance with current authorised records retention and disposal authorities), accountability, and community expectations. • Decommissioning of systems includes retention and disposal requirements for records, information and data contained in the system.
2.6 Records, information and data are sustained through system and service transitions by strategies and processes specifically designed to support business and accountability.	• Documented migration strategy. • Migrating records and metadata from one system to another is a managed process which results in trustworthy and accessible records. • Portability of records and information is assessed in cloud service or similar arrangements. • Adequate system documentation is maintained.

Principle 3: Records and information are well managed

Effective management of records, information and data underpins trustworthy, useful and accountable records and information, which are accessible and retained for as long as they are needed. This management extends to records, information and data in all formats, in all business environments, and in all types of systems.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
3.1 Records, information and data are routinely created and managed as part of normal business practice.	• Policies, business rules and procedures articulate/document staff requirements and responsibilities for the creation, capture and management of records of business operations and processes. • Assessments or audits demonstrate that systems operate routinely and records and metadata are created and captured. • Exceptions to routine operations that affect information integrity, useability or accessibility are identified, resolved and documented.
3.2 Records, information and data are managed to ensure they are reliable and trustworthy.	• Adequate metadata is created and captured to ensure meaning and context is associated with the record. • System audits are undertaken to test controls of systems and to verify records and information integrity and trustworthiness. • Policies, business rules, procedures and other control mechanisms are in place to ensure accuracy and quality of records created, captured and managed.
3.3 Records, information and data are identifiable, retrievable and accessible for as long as they are required.	• System testing is able to verify that systems can identify, retrieve and produce records which are viewable and understandable. • Adequate metadata is created and captured to ensure that records are identifiable and accessible. • Data and metadata are used and shared with consideration of Indigenous Data Sovereignty principles and Indigenous Cultural and Intellectual Property protocols. • Data is managed to facilitate effective use and reuse of information.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
3.4 Records, information and data are protected from unauthorised or unlawful access, destruction, loss, deletion or alteration.	• Records are stored in accordance with the requirements of the *Standard on the physical storage of State records*, the NSW Government Data Strategy and the NSW Government Cloud Policy. • Information security and protection mechanisms, such as those outlined in the the NSW Cyber Security Policy, the NSW Government Information Classification, Labelling and Handling Guidelines and the Australian Protective Security Policy Framework, are in place. • Records are protected wherever they are located, including in transit and when outside the workplace. • Access, security and user permissions for systems managing records, information and data are documented and implemented. • System audits are able to test that access controls are implemented. • State Records NSW is notified when damage to records affects the integrity of records, or when records are lost or unlawfully accessed, destroyed, deleted or altered. • The Privacy Commissioner and affected individuals are notified of eligible data breaches in accordance with the Mandatory Notification of Data Breach Scheme.

Minimum compliance requirements	**Examples of how a public office can demonstrate compliance with the requirement**
3.5 Access to records, information and data is managed appropriately in accordance with legal and business requirements.	• Access to records is provided in accordance with such instruments as the *Privacy and Personal Information Protection Act 1998* (‘PPIP Act’), *the Government Information (Public Access) Act 2009 (‘GIPA Act’)* and the *State Records Act 1998.* • Policy, business rules and procedures identify how access to records, information and data is managed. • Assessments confirm that access is in accordance with the organisation’s policy, business rules and procedures. • Records that are 20 years or older are covered by a closed to public access direction where required. Closed to public access directions are registered with Museums of History NSW in accordance with Part 6 of the *State Records Act 1998*. • The Privacy Commissioner and affected individuals are notified of eligible data breaches in accordance with the Mandatory Notification of Data Breach Scheme.
3.6 Records, information and data are kept for as long as they are needed for business, legal and accountability requirements.	• Policy, business rules and procedures identify how the retention and disposal of records, information and data is managed. • Records, information and data are sentenced according to current authorised retention and disposal authorities. • Facilitative or duplicate records, information and data are sentenced according to normal administrative practice provisions where appropriate. • Authorised disposal activities are routinely conducted to minimise over-retention of records, information and data. • Records required as State archives are routinely transferred to Museums of History NSW when no longer in use for official purposes.

Minimum compliance requirements	Examples of how a public office can demonstrate compliance with the requirement
3.7 Records, information and data are systematically and accountably destroyed when legally appropriate to do so.	• Policy, business rules and procedures identify how the destruction of records and information is managed, including deletion of data. • Disposal is in accordance with current authorised records retention and disposal authorities. • Disposal of records is documented and authorised. • Organisation can account for the disposal of records or information in accordance with legal obligations and accountability requirements.