SRC Standard

STATE RECORDS MANAGEMENT

A Standard for State Organisations

State Records Commission
Perth, Western Australia
June 2020

PURPOSE

The purpose of this Standard is to define principles and standards governing records management by State organisations.

This Standard supersedes *SRC Standard 1: Government Recordkeeping,* 2002; *SRC Standard 2: Recordkeeping Plans,* 2002; *SRC Standard 3: Appraisal of Records,* 2002; *SRC Standard 4: Restricted Access Archives,* 2002; *SRC Standard 6: Outsourcing,* 2002; *SRC Standard 7: State Archives Retained by Government Organisations,* 2016; and *SRC Standard 8: Managing Digital Information,* 2016.

SCOPE

The principles and minimum compliance requirements in this Standard apply to all State organisations as defined in Section 3 of the *State Records Act 2000*.

The Standard covers all State records of information created and retained however recorded and in any format.

AUTHORITY

This Standard is issued under Section 61(1) of the *State Records Act 2000* and has been approved by the State Records Commission (SRC) in accordance with Section 61(2) of the Act.

DEFINITIONS

Refer to the *Glossary of Terms* produced by the State Records Office of Western Australia (SRO) and available on the SRO website.

Principle 1 – Creation and Management

Organisations create, capture and manage records of information which properly and adequately record the performance of the organisation's functions and supports business operations.

Minimum compliance requirements:

1. Organisations have a Records Management Plan directing how records of information shall be created, managed and kept in accordance with legislative and business requirements.
2. Accountability and responsibility for approving, implementing and regularly reviewing Records Management Plans are assigned by the organisation.
3. All employees, including contractors and third-party providers engaged in outsourcing arrangements, comply with the Records Management Plan.
4. Records of information are protected, preserved and stored on appropriate media to ensure ongoing usability, in environmental conditions appropriate to format.
5. Migrated, converted or reproduced records of information are as authentic, reliable and usable as the original source records from which they are created.
6. Effective security and authentication controls exist to keep records of information safe from intentional or unintentional damage and unauthorised access, tampering or alteration.

Examples of compliance:
• Organisation has an existing Record Keeping Plan with plans to review it within five years of being approved by the State Records Commission and replace it with a Records Management Plan • Organisation has a current Records Management Plan endorsed by Senior Management and can provide documentation regarding the organisation's business system/s, retention and disposal arrangements, policies, practices and processes, on request • Organisation reviews its Records Management Plan every five years and regularly updates documentation when necessary • Organisation uses relevant guidelines, templates and specifications provided by the SRO to inform risk management planning, and address activities such as storage conditions, migration strategies, vital records, disaster recovery, backup of digital records and applicable security and access controls • Contracts with third party providers address records of information created during the life of the contract including the control, access, ownership and return of those records of information • Organisation has staff training in place

Principle 2 – Retention and Disposal

All records of information have a minimum retention period for which they must be kept. Some records of information have continuing value and are to be kept permanently as State archives.

Minimum compliance requirements:

1. Records of information are kept for the minimum periods outlined in the appropriate retention and disposal authorities and any applicable legislation.
2. State archives are identified for permanent retention through approved retention and disposal authorities.
3. Legal destruction of records of information which are not State archives, and are no longer required for business purposes, is regularly conducted in accordance with appropriate retention and disposal authorities.

Examples of compliance:

- Organisation implements Disposal Authorities approved by the State Records Commission
- Organisation has a retention and disposal program in place to regularly and securely dispose of records of information, regardless of format, so that they cannot be reconstructed or recovered
- Organisation uses relevant guidelines and advice provided by the SRO to implement disposal programs

Principle 3 – Discovery and Access

Organisations must be able to efficiently and effectively locate and retrieve records of information when required for business purposes and in order to allow discovery and provide a right of access to government information.

Minimum compliance requirements:

1. Appropriate controls are in place to identify and name all government records of information.
2. All records of information, including those created by contractors and third-party providers engaged in outsourcing arrangements, are accessible when required.
3. State archives must be open for public access at some point in their life.

Examples of compliance:

- Organisation has standards for titling records of information
- Organisation uses relevant guidelines and advice provided by the SRO to provide access to records of information for government and the public
- Access to restricted access archives is administered by the organisation
- Contracts with third-party providers contain provision for access to records of information