Western Australia

State Records Act 2000

State Records Principles and Standards 2016

As at 22 Jun 2016 Version 00-a0-02
Published on www.legislation.wa.gov.au

Western Australia

State Records Principles and Standards 2016

Contents

State Records Principles and Standards 2016

1. Citation

These principles and standards may be cited as the *State Records Principles and Standards 2016*.

2. Commencement

These principles and standards come into operation on the day after the day on which they are published in the *Government Gazette*.

3. Government record keeping

SRC Standard 7	State Archives Retained by Government Organizations
SRC Standard 8	Managing Digital Information

STATE RECORDS COMMISSION

SRC Standard 7

State Archives Retained by Government Organizations

A Recordkeeping Standard for Government Organizations

State Records Commission of WA
Perth, Western Australia
June 2016

STATE RECORDS ACT 2000

STATE RECORDS COMMISSION

SRC STANDARD 7—STATE ARCHIVES RETAINED BY GOVERNMENT ORGANIZATIONS

Table of Contents

STATE RECORDS ACT 2000

STATE RECORDS COMMISSION

SRC STANDARD 7—STATE ARCHIVES RETAINED BY GOVERNMENT ORGANIZATIONS

PURPOSE

The purpose of this Standard, established under section 61(1) of the *State Records Act 2000*, is to provide for a government organization to retain a State archive beyond the compulsory transfer period, and to ensure the safe storage, preservation, handling and access to a State archive retained by a government organization with State Records Commission approval.

This Standard *supersedes SRC Standard 5: Compulsory Transfer of Archives, 2002* and *SRC Standard 7: Storage of State Archives retained by State Organizations* through an approved Recordkeeping Plan, 2008.

BACKGROUND

Under section 32(1) of the *State Records Act 2000*, a government organization must transfer a State archive that is under its control to the State archives collection when it becomes twenty-five (25) years old, unless the organization's Recordkeeping Plan says otherwise.

If an organization needs to retain custody of a State archive beyond the compulsory transfer period, the organization must apply and obtain approval, via its Recordkeeping Plan, from the State Records Commission. In order to approve such custodial arrangements, the State Records Commission must be assured that the archive will be maintained in appropriate conditions and will remain accessible in accordance with the relevant provisions of the *State Records Act 2000*.

Archives in digital formats and some analogue (physical) formats (particularly audio-visual) have retention periods greater than one **generation of technology.**

These items must be preserved and remain accessible for use either using open standard, non-proprietary formats, or using equipment and software able to access the formats. The minimum compliance requirements outlined in this Standard aim to ensure that government organizations implement controls and practices that will support the proper management of State archives that remain in their custody.

Note: An organization may request to transfer a State archive to the State archives collection at any time before it becomes 25 years old. If the Director of State Records is unable to accept the transfer, the Director will advise accordingly.

SCOPE

The principles and minimum compliance requirements in this Standard apply to all government organizations as defined in the *State Records Act 2000*.

This Standard does not apply to government records that are not State archives.

DEFINITIONS

Refer to the Glossary of Terms produced by the State Records Office of Western Australia available on the State Records Office website.

PRINCIPLE 1—APPLICATION TO RETAIN STATE ARCHIVES

GOVERNMENT ORGANIZATIONS ARE TO APPLY TO RETAIN A STATE ARCHIVE BEYOND THE COMPULSORY TRANSFER PERIOD OF 25 YEARS

Rationale

In general, records have a currency or administrative use of 7 to 10 years. Some records may carry a business use of 20 years or more. If records are designated as State archives, the Act requires they are to be transferred to the State archives collection when they are 25 years old to be kept in perpetuity.

A government organization may determine that it has a business need to retain a State archive for official purposes and that the State archive should not be transferred to the State archives collection.

In applying to retain a State archive beyond the compulsory transfer period, the State Records Commission is to be apprised of the organization's reasons for keeping the State archive and provided with assurance that the State archive will be properly kept and accessible.

The decision to retain a State archive beyond the compulsory transfer period is to be reviewed every five years as part of the review of the organization's Recordkeeping Plan.

Minimum Compliance Requirements

The government organization's Recordkeeping Plan must provide evidence to adduce that the State archive that is not to be transferred—

1. Is required by the organization for ongoing official purposes beyond the compulsory transfer period (i.e. the justification for non-transfer).
2. Is identified in an approved Disposal Authority.
3. Will be kept in accordance with Principles 2 to 7 in this Standard.

PRINCIPLE 2—ENVIRONMENTAL CONDITIONS

GOVERNMENT ORGANIZATIONS ENSURE THAT STATE ARCHIVES ARE STORED IN ENVIRONMENTAL CONDITIONS APPROPRIATE TO THEIR FORMAT

Rationale

State archives are to be stored in areas or facilities that are suitable for archival storage in accordance with international and national standards. State archives require storage in controlled conditions to ensure their continued usability.

Details of minimum requirements for environmental conditions for the storage of archives can be found in the Archival Storage Specification produced by the State Records Office, available on the State Records Office website.

Minimum Compliance Requirements

Government organizations must ensure that—

1. All premises and facilities used for the storage of State archives maintain environmental conditions that meet those described in the Archival Storage Specification.

2. The location of storage areas and storage facilities supports the preservation of State archives; minimizes risks; and enables timely and efficient retrieval.

PRINCIPLE 3—STORAGE MECHANISMS

GOVERNMENT ORGANIZATIONS ENSURE THAT STATE ARCHIVES ARE STORED APPROPRIATE TO THEIR FORMAT

Rationale

State archives must be stored on shelving, in enclosures and on media that contributes to their ongoing preservation and accessibility.

Organizations must ensure that any digital State archives are stored on media appropriate for long-term viability. Technology dependent media must be subject to regular integrity checks to ensure the information remains intact and usable. Technology dependent media must be monitored and periodically refreshed to prevent data loss through media degradation and format obsolescence.

Details of minimum requirements for storage used for archives in a variety of formats can be found in the Archival Storage Specification produced by the State Records Office.

Minimum Compliance Requirements

Government organizations must ensure that—

1. Storage used for State archives is in compliance with those described for each format type in the Archival Storage Specification.

2. Technology dependent media is of a format that remains usable by the government organization.

PRINCIPLE 4—SECURITY AND DISASTER MANAGEMENT

GOVERNMENT ORGANIZATIONS ENSURE THAT STATE ARCHIVES ARE SAFEGUARDED AND SECURE

Rationale

State archives are to be stored securely, with steps taken to manage any potential threat to their security, including appropriate authentication controls for access. State archives must be protected from intentional or unintentional damage, unauthorized tampering, or alteration. Organizations must take special care to ensure their information systems are secure, reliable and capable of maintaining information that is acceptable for business, legal, audit and other purposes.

Minimum Compliance Requirements

Government organizations must ensure that—

1. Protocols are in place that determine who within the organization has responsibility for managing authorized access to its State archives.

2. A disaster management plan is in place, as per the requirements of SRC Standard 2: Recordkeeping Plans, Principle 4—Preservation.

3. Procedures are in place to identify and respond to incidents which have the potential to cause damage or attempted security breaches of storage areas and of systems that manage and store archives.

4. Access to archives is secured and auditable.

5. Copies or backups of archives held for disaster recovery purposes are secured to the same level as the originals.

PRINCIPLE 5—ACCESS

GOVERNMENT ORGANIZATIONS ENSURE THAT STATE ARCHIVES ARE ACCESSIBLE

Rationale

Under Part 6 of the *State Records Act 2000*, the public has a right of access to State archives not in the State archives collection, in accordance with the stipulations of the Act. Any right that a person may have to be given access to a restricted access archive is to be determined under the *Freedom of Information Act 1992*.

Organizations must be able to locate and retrieve State archives when required for access. Computer systems and technology dependent media which hold archives must be available for authorized access, including the ability to run an application on appropriate hardware and operating systems for the purpose of accessing information held in State archives.

Suitable services must be made available for the secure and protected access to archives within the organization.

Minimum Compliance Requirements

Government organizations must ensure that—

1. Policies and procedures are in place that enable the provision of public access to State archives of the organization in accordance with section 45 of the *State Records Act 2000*.

2. The public has access to information that identifies State archives in the custody of the organization, subject to any written law or conditions that have been outlined in the organization's Recordkeeping Plan.

PRINCIPLE 6—CONTROL

GOVERNMENT ORGANIZATIONS ENSURE THAT STATE ARCHIVES ARE CONTROLLED

Rationale

An organization with custody of State archives must have a control system to help manage, locate, retrieve, describe and make accessible the State archives that it holds.

Information about the State archives in the custody of organizations must be able to be quantified and this information preserved.

Minimum Compliance Requirements

Government organizations must ensure that—

1. State archives are registered in a system to identify and provide control of such information.

PRINCIPLE 7—PRESERVATION

GOVERNMENT ORGANIZATIONS ENSURE THAT STATE ARCHIVES ARE PRESERVED FOR THE LONG TERM AND ENSURE THAT BOTH ANALOGUE AND DIGITAL FORMATS REMAIN USABLE

Rationale

State archives require preservation actions to ensure they remain usable for the long term. Organizations must ensure that they take appropriate actions, whether passive or active, to preserve these items.

Incorrect handling of State archives may degrade or destroy the integrity of an archive. For the purpose of ensuring safe custody and protecting the condition of a State archive, organizations are to institute appropriate handling protocols. Where appropriate, archives may be reproduced for access purposes to assist in maintaining the originals in good condition.

Archives have a life greater than one generation of technology. Therefore, information must be preserved and remain usable by migrating or rendering to current file formats, or to open standard, non-proprietary formats, whenever applications are upgraded or a new format comes into more common use.

In conducting migration activities, it is the responsibility of the organization to define the essential characteristics of digital records that must not change as a result of migration processes. Organizations must also conduct testing to check

that content and essential characteristics of digital records are not compromised by migration processes.

Any organization undertaking a technology upgrade, or adopting new or updated business systems, must ensure that the migration of information into the new system is undertaken so that the information is usable.

Minimum Compliance Requirements

Government organizations must ensure that—

1. State archives in digital format are stored in an appropriate file format.
2. Systems planning, design and implementation includes the provision for conversion or migration of the previous (or legacy) systems data.
3. Strategies and procedures for the preservation and usability of digital information are developed, implemented and reviewed at regular intervals and staff are aware of and trained in these processes.
4. Protocols are in place for the handling of State archives that encourage proper handling practices.
5. Cleaning and repair of State archives which are fragile or show signs of degradation is only carried out in consultation with the State Records Office.
6. The process for digitization of State archives does not damage the original items.

For further information regarding this Standard contact—

State Records Office of WA

Phone: 9427 3600

Email: sro@sro.wa.gov.au

STATE RECORDS COMMISSION

SRC Standard 8

MANAGING DIGITAL INFORMATION

A Recordkeeping Standard for State Organizations

State Records Commission of WA
Perth, Western Australia
June 2016

STATE RECORDS ACT 2000

STATE RECORDS COMMISSION

SRC STANDARD 8—MANAGING DIGITAL INFORMATION

Table of Contents

STATE RECORDS ACT 2000

STATE RECORDS COMMISSION

SRC STANDARD 8—MANAGING DIGITAL INFORMATION

PURPOSE

The purpose of this Standard, established under section 61 of the *State Records Act 2000*, is to describe requirements that must be satisfied in Recordkeeping Plans for State organizations to demonstrate good practice digital recordkeeping. It is not the intention of this document to prescribe that State organizations must move to digital recordkeeping, but to provide Principles for those that do keep information in a digital format.

This Standard supersedes *SRC Standard 8: Digital Recordkeeping, 2008*.

BACKGROUND

State organizations create many state records and information in digital format. Managing digital information differs from managing physical information. At the lowest level, digital information is made up of binary encoded data that requires software to reveal its contents. Digital information is stored on a variety of digital media that is easily damaged and may be prone to obsolescence. Consequently, the storage of digital information both in terms of storage media and the file formats in which they are kept, must be managed with methods to ensure that the information is available and sufficient to meet accountability, business and archival requirements. In managing digital information, State organizations must also comply with the *State Records Act 2000*.

Digital information is any digitally produced or stored record of information within the meaning of section 3 of the *State Records Act 2000* and must be captured as evidence of business activity and stored into recordkeeping systems

along with metadata that describes their content, structure and context. These requirements are set out in *SRC Standard 1: Government Recordkeeping* and *SRC Standard 2: Recordkeeping Plans. Digital information* must be managed to remain usable for as long as it is required. Access to digital information is regulated through legislation such as the *State Records Act 2000* and *Freedom of Information Act 1992*. Close attention to security mechanisms is essential to prevent unauthorized access or tampering with digital information. State organizations must plan for the recovery of lost data in the event of a disaster—loss of digital information can be crippling to the reconstruction of business activity.

Given the rapid obsolescence of technology, organizations should plan the preservation of digital information according to its required period of retention. Digital information that is to be retained on a long term basis by a State organization, or is to be transferred to the State archives collection, requires active and ongoing preservation to ensure its usability.

Digital information identified as State archives must be kept in a software file format and on media that is both viable and usable until it is transferred into the State archives collection.

Digital information of temporary value must be destroyed securely in accordance with an approved disposal authority and in such a way that it cannot be reconstructed.

SCOPE

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

The Standard describes specific requirements for the good practice management of digital information that is either born digital or has been created as a consequence of the digitization of physical source records.

DEFINITIONS

Refer to the Glossary of Terms produced by the State Records Office of Western Australia available on the State Records Office website.

PRINCIPLE 1—MANAGING DIGITAL INFORMATION

STATE ORGANIZATIONS ENSURE THAT ALL DIGITAL INFORMATION IS MANAGED APPROPRIATELY

Rationale

Digital information includes all types of business information created and maintained electronically. This may include (but is not limited to): email, web sites, databases, application systems, word processed documents, spreadsheets, social media and digital reproductions of physical records. State organizations should develop policies, procedures and business solutions for capturing this information and managing it for as long as it is required in corporate recordkeeping compliant systems.

Minimum Compliance Requirements

State organizations must ensure that—

1. All matters relating to the management of digital information are contained within their Recordkeeping Plans.

2. In developing policies, procedures and solutions for the management of digital information, reference is made to relevant State Records Commission Standards and Guidelines produced by the State Records Office.

PRINCIPLE 2—APPRAISAL, RETENTION AND DISPOSAL OF DIGITAL INFORMATION

STATE ORGANIZATIONS ENSURE THAT DIGITAL INFORMATION IS APPRAISED AND ITS RETENTION AND DISPOSAL IS MANAGED IN ACCORDANCE WITH APPROVED DISPOSAL AUTHORITIES

Rationale

Digital information created by State organizations during the course of business is a State record for the purposes of the *State Records Act 2000*. Digital information must therefore be appraised in accordance with *SRC Standard 3: Appraisal of Records, Principle 1—Appraisal*; and its retention and disposal managed in accordance with *SRC Standard 2: Recordkeeping Plans, Principle 5—Retention and Disposal*.

Digital information needs to be kept until it is no longer required for any purpose. There are three general reasons information needs to be kept, namely—

- to support the efficient conduct of business;
- to meet the requirements of legislation and accountability; and
- to meet the expectations of the community.

State organizations should prepare strategies for efficient digital preservation solutions in accordance with Principle 4—Storing Digital Information. Digital information that has been identified as State archives must be held in software file formats with the appropriate metadata and on media that is both viable and usable until such time as it is transferred to the State archives collection.

Minimum Compliance Requirements

State organizations must ensure that—

1. Digital information is appraised in accordance with *SRC Standard 3: Appraisal of Records, Principle 1—Appraisal*.
2. The retention and disposal of digital information is managed in accordance with *SRC Standard 2: Recordkeeping Plans, Principle 5—Retention and Disposal*.
3. Destruction of digital information is authorized and conducted using appropriately secure methods of destruction, ensuring the information cannot be reconstructed.

PRINCIPLE 3—SECURITY OF DIGITAL INFORMATION

STATE ORGANIZATIONS ENSURE THAT EFFECTIVE SECURITY AND AUTHENTICATION CONTROLS EXIST TO ENSURE DIGITAL INFORMATION IS SAFE FROM INTENTIONAL OR UNINTENTIONAL DAMAGE AND UNAUTHORIZED TAMPERING OR ALTERATION

Rationale

Adequate security is essential for all State records. When implementing information systems, State organizations must take special care to ensure they are secure, reliable and capable of producing records that are acceptable for business, legal, audit and other purposes.

The nature of digital information can make it susceptible to alteration or deletion, whether intentionally or unintentionally. Alterations to digital information can be virtually undetectable, undermining its evidential value as a record. Digital information is easily copied and the taking of copies can be undetectable, potentially leading to unauthorized access to confidential and personally or commercially sensitive data. Information Security and Computer Security are both equally important in planning for secure digital information stores and application systems. Security controls should be in place at all levels, including physical, network, operating system and application level, for production and development systems as well as backup data.

State organizations must recognize that data stored offshore is potentially beyond the control of the State government, and must undertake appropriate risk assessments of the data before selecting storage or data centres, whether onshore or offshore. State organizations must also ensure that data stored with an outsourced provider meets the requirements of *SRC Standard 6: Outsourcing*.

Minimum Compliance Requirements

State organizations must ensure that—

1. Information systems are protected to best practice security standards.
2. Procedures are in place to identify and respond to incidents or attempted security breaches of systems that create or store digital information.
3. Systems and protocols are in place to prevent unauthorized access to, or alteration of, digital information and ensure its authenticity.
4. Procedures ensure that security and authentication mechanisms such as encryption and digital rights management (DRM) do not inadvertently make digital information inaccessible in the long term.
5. Access to digital information is secured and auditable.

6. A risk assessment is undertaken before storing information or application systems offsite or offshore.

PRINCIPLE 4—STORING DIGITAL INFORMATION

STATE ORGANIZATIONS ENSURE THAT DIGITAL INFORMATION IS STORED ON APPROPRIATE MEDIA TO ENSURE ITS ONGOING USABILITY

Rationale

Digital information is vulnerable to loss, destruction, unauthorized copying and modification. To ensure the ongoing protection of digital information, State organizations require efficient and effective means of maintaining, handling, securing, and storing digital information over time. Policies, procedures and effective mechanisms for the storage of digital information should be an integral component of an organization's recordkeeping framework. Recordkeeping Plans should contain recovery and restoration procedures for digital information in compliance with *SRC Standard 2: Recordkeeping Plans, Principle 4—Preservation*.

The storage arrangements for digital information, and the media type on which it is stored, should depend on risk assessments of the information and business requirements. To ensure the integrity, reliability and usability of information, policy and procedures are required for the—

- Selection of storage media and devices;
- Storage locations and conditions;
- Security;
- Refreshment of media;
- Migration of data; and
- Integrity checks.

Where information is held in an archive file format, organizations must ensure that these formats as well as the media they are stored on are able to be read for as long as the record or data is required to be held.

Note: Backups are suitable for disaster recovery but are not a viable long term storage solution.

Minimum Compliance Requirements

State organizations must ensure that—

1. Digital information is stored on appropriate and durable media to ensure the information remains usable for as long as required.
2. Digital storage devices are subjected to regular integrity checks and periodically refreshed to prevent data loss through media degradation or obsolescence.
3. Backup or 'IT archive' file formats remain usable for as long as required.
4. Risk assessments are conducted on information and data prior to the selection of storage locations.

PRINCIPLE 5—DIGITIZATION

STATE ORGANIZATIONS ENSURE THAT DIGITIZED INFORMATION IS AS AUTHENTIC, RELIABLE AND USABLE AS THE SOURCE MATERIAL FROM WHICH IT IS CREATED

Rationale

Digitization is the creation of a digital reproduction or likeness of an analogue file (printed paper, photograph, audio tape, etc). Whether a digital reproduction can stand in place of source material as proof of a business transaction, or as evidence, depends upon its authenticity, integrity, reliability and usability.

If a reproduction is intended to serve the same purpose as the source material, then the reproduction will need to be as usable, authentic and as reliable as the original. Reproductions are subject to the same requirements as any other digital information and therefore a State organization must have sufficient confidence in its digitization procedures to certify the authenticity of the reproductions. Where the digital reproductions need to be kept for the long term, they must be preserved in the file formats identified in the Digitization Specification produced by the State Records Office. The conditions for the process of creating

digital reproductions of documents which involves the destruction of the source record are outlined in the General Disposal Authority for Source Records.

Where destruction of the source material is contemplated, State organizations must ensure that a risk assessment has been performed identifying risks and risk minimization strategies and that this risk assessment has been included in their Recordkeeping Plans.

Minimum Compliance Requirements

State organizations must ensure that—

1. Any digitization which involves the destruction of source records is undertaken within the framework of the General Disposal Authority for Source Records.

2. Policy and procedures comprehensively describe digitization, security and quality assurance practices.

RELATED DOCUMENTS

Standards Australia Limited and Standards New Zealand, Australian/New Zealand Standard AS/NZS ISO 16175 Information and documentation—Principles and functional requirements for records in electronic office environments. Standards Australia Limited, Sydney; Standards New Zealand, Wellington, 2012.

For further information regarding this Standard please contact—
State Records Office of WA
Phone: 9427 3600
Email: sro@sro.wa.gov.au

Notes

[1] This is a compilation of the *State Records Principles and Standards 2002.*

Compilation table

Citation	Gazettal	Commencement
State Records Principles and Standards 2016	21 Jun 2016 p. 2211-30	22 Jun 2016 (see cl. 2)