WESTERN AUSTRALIAN GOVERNMENT Gazette
ISSN 1448-949X PRINT POST APPROVED PP665002/00041

PERTH, FRIDAY, 29 FEBRUARY 2008 No. 37 SPECIAL

PUBLISHED BY AUTHORITY JOHN A. STRIJK, GOVERNMENT PRINTER AT 3.45 PM

State Records Act 2000

State Records (Digital Recordkeeping) Standard 2008

Made by the State Records Commission under section 61 of the Act.

1. Citation

This standard may be cited as the *State Records (Digital Recordkeeping) Standard 2008*.

2. Commencement

This standard comes into operation on the day after the day on which it is published in the *Government Gazette*.

3. Government record keeping

SRC Standard 8 Digital Recordkeeping

Dated: 29 January 2008.

COLIN MURPHY, Chair.

KANDY JANE HENDERSON, Member.

CHRIS FIELD, Member.

JOHN LIGHTOWLERS, Member.

STATE RECORDS COMMISSION

SRC Standard 8

DIGITAL RECORDKEEPING

A Recordkeeping Standard for State Organizations

State Records Commission of WA
Perth, Western Australia
February 2008

SRC STANDARD 8 —DIGITAL RECORDKEEPING

TABLE OF CONTENTS

SRC STANDARD 8 —DIGITAL RECORDKEEPING

DEFINITIONS

Application system—organized collection of hardware and software which stores, processes and supplies access to organizational information.

Appraisal—is the process of determining which records are to be retained as archives and which will be destroyed.

Archival value—continuing or permanent value warranting preservation.

Archives—records that have been appraised as having archival value.

Business continuity planning—the process of identifying, preventing or preparing for events that may interrupt business activities to protect critical business processes from the effects of major failures or disasters.

Computer security—the process of enforcing restrictions of access to a computer system (both hardware and software) so that users of the system may only perform pre-defined actions.

Content—that which conveys information, e.g. text, data, symbols, numerals, images, sound and vision.

Context—the background information that enhances understanding of technical and business environments to which the records relate e.g. metadata, application software, logical business models, and the provenance (i.e. address, title, link to function or activity, agency, program or section).

Digital record—any record of information within the meaning of Section 3 of the *State Records Act 2000* that exists in binary form and that requires combinations of computer hardware and software to be read and understood.

Digitization—converting paper and other media in existing collections to digital form.

Disaster recovery—preventative measures that may use redundant hardware, software, replicated digital records and other facilities to ensure that a State organization can restore digital records and related business operations as quickly as possible following a disaster.

Disposal—the removal of records from the organization and their subsequent destruction or permanent retention as State archives.

Digital Rights Management (DRM)—technology used to control or limit access to and use of digital media.

Framework—a unified view of the program elements needed to realize the implementation of an organizational goal, service or application. In the case of digital recordkeeping, these elements consist of role and responsibility assignments, principles, policies, procedures and compliance arrangements.

Government organization—an organization listed in Schedule 1 or Schedule 3 of the *State Records Act 2000*.

Government record—a record created or received by a government organization, a government employee, or contractor in the course of working for the organization.

Information security—the protection of data from unauthorized use, misuse, deletion or modification.

Integrity check—a mechanism to verify that the present state of data does not involve tampering, modification or bit loss in a manner that compromises authenticity, completeness and reliability.

Long-term—greater than one generation of technology.

Metadata—data describing the context, content and structure of records and their management over time.

Migration—the act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability. Migration involves a set of organized tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another.

Nearline—nearline storage of digital records means the records are contained on removable digital storage media, but remain relatively accessible through automated systems connected to the network.

Offline—digital records are considered offline when they exist on a system or storage device that is not directly accessible through a State organization's network and on media which has to be inserted manually by an operator to become available nearline or online.

Online—digital records are considered online when they are available for immediate access via a storage device that is turned on and connected to a network either directly or indirectly.

Open Standard—a standard that is publicly available for review and use.

Preservation—the process and operations involved in ensuring the technical and intellectual survival of authentic records over time.

Record—means any record of information however recorded and includes—

(a) any thing on which there is writing or Braille;

(b) a map, plan, diagram or graph;

(c) a drawing, pictorial or graphic work, or photograph;

(d) any thing on which there are figures, marks, perforations, or symbols, having a meaning for persons qualified to interpret them;

(e) any thing from which images, sounds or writings can be reproduced with or without the aid of anything else; and

(f) any thing on which information has been stored or recorded, either mechanically, magnetically or electronically.

Recordkeeping system—a system to capture, maintain and provide access to records over time that displays features for ensuring authentic, reliable, complete and usable records that function as evidence of business transactions.

Recordkeeping systems include—

1. a set of authorized policies, assigned responsibilities, delegations of authority, procedures and practices; policy statements, procedures manuals, user guidelines and other documents which are used to authorize and promulgate the policies, procedures and practices;
2. the records themselves;
3. specialized information and records systems used to control the records; and
4. software, hardware and other equipment, and stationery.

Refreshment—the transfer of digital files to new media on a regular basis.

State organization—a parliamentary department or a government organization.

State record—a parliamentary record or a government record.

Structure—the appearance and arrangement of a record's content (e.g. the relationships between fields, entities, language, style, fonts, page and paragraph breaks, links and other editorial devices).

Temporary value—records which can be legally destroyed within an approved time frame because they lack archival value.

Vital records—records that are essential for the ongoing business of a State organization, without which it could not continue to function effectively.

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.

BACKGROUND

Western Australian State government organizations create many government records in digital format. Requirements for managing digital records can be different from traditional records. At their lowest level, digital records are made up of binary encoded data that requires software to reveal their contents. Digital records exist on a variety of electronic media that are easily damaged and prone to technology obsolescence. Consequently, the storage of digital records must be managed with methods to ensure that they are available and sufficient to meet accountability, business and archival requirements. In managing digital records, State organizations must also comply with the *State Records Act 2000*.

Digital records are records as defined in 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 State Records Commission (SRC) Standards 1 and 2. Digital records must be managed to remain accessible for as long as they are required. Access provisions to digital records are regulated through legislation such as the *State Records Act 2000* and *Freedom of Information Act 1992*. Because digital records can be easily modified, their security is very important. State organizations should plan for the recovery of lost data in the event of a disaster – loss of digital records can be crippling.

Given the rapid obsolescence of digital technology, organizations should plan for the long-term preservation of digital records. Digital records that are to be retained on a long-term basis by a State organization require preservation to ensure their ongoing accessibility.

Digital records of temporary value must be destroyed securely in accordance with an approved disposal authority and in such a way that they 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 records that are either born digital or have been created as a consequence of digitization of source records. Such requirements arise from the differences that exist between digital records and traditional records as information sources and the need to ensure that such differences are recognized in the making and managing of digital records.

Principle 1—Managing Digital Records

State organizations ensure that all types of digital records are managed appropriately.

Rationale

Digital records include all types of records that are created and maintained electronically. These records may include (but are not limited to): email, web sites, database applications, word processed documents, spreadsheets and digitized reproductions of documents. State organizations should develop policies, procedures and business solutions for capturing these records and managing them for as long as they are required in a corporate recordkeeping compliant system.

Minimum Compliance Requirements

State organizations must ensure that—

1. All matters relating to management of digital records is contained within their Recordkeeping Plan.
2. In developing policies, procedures and solutions for digital recordkeeping, reference is made by State organizations to relevant Guidelines produced from time to time by the State Records Office.

Principle 2—Appraisal, Retention and Disposal of Digital Records

State organizations ensure that digital records are appraised and their retention and disposal is managed in accordance with approved retention and disposal authorities.

Rationale

Digital records created by State organizations during the course of business are State records for the purposes of the *State Records Act 2000*. Digital records must therefore be appraised in accordance with SRC Standard 3, Principle 1—Appraisal, and their retention and disposal managed in accordance SRC Standard 2, Principle 5—Retention and Disposal.

Digital records need to be kept until they are no longer required for any purpose. There are three general reasons digital records need 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.

The principle of appraisal applies to digital records with particular attention directed to—

- records of significant operations; and
- records that document the rights and obligations of the State or of private individuals.

Digital records that have been identified as State archives are to be retained within the State organization.* State organizations should prepare strategies for efficient digital preservation solutions in accordance with Principle 5— Preserving Digital Records.

Destruction of digital records must ensure that the record cannot be reconstructed.

Minimum Compliance Requirements

State organizations must ensure that—

1. Digital records are appraised in accordance with SRC Standard 3, Principle 1.
2. The retention and disposal of digital records is managed in accordance with SRC Standard 2, Principle 5.
3. The authorized destruction of digital records is conducted using appropriately secure methods of destruction.

* *The State Records Office expects to have digital archives facilities in the future enabling it to accept digital archives into its custody.*

Principle 3—Security of Digital Records

State organizations ensure that effective security and authentication controls exist to ensure digital records are safe from intentional or unintentional damage and unauthorized tampering or alteration.

Rationale

Security is essential for all State records. The nature of digital records means that, in the absence of appropriate safeguards, it is relatively easy to alter or delete information – whether intentionally or unintentionally. Alterations to digital records can be virtually undetectable, undermining their evidential value as records. Two kinds of security are important in planning for secure digital records and systems - Information Security and Computer Security.

When implementing 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. Security measures should be implemented for all systems.

Minimum Compliance Requirements

State organizations must ensure that—

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

Principle 4—Storing Digital Records

State organizations ensure that digital records are stored on appropriate media to ensure their ongoing accessibility.

Rationale

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

Whether digital records are kept online, nearline or offline should depend on assessments of recordkeeping and business requirements. To ensure the completeness, reliability and usability of records, policy, procedures and guidelines are also required for—

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

A storage repository intended to provide for long-term storage of digital records should have a written preservation policy. Quality control, security and environmental control are important areas of good practice repository management.

Minimum Compliance Requirements

State organizations must ensure that—

1. Digital records are stored on appropriate media.
2. Digital storage devices are subjected to regular integrity checks.
3. Digital storage media are monitored and periodically refreshed to prevent data loss through media degradation and obsolescence.
4. Digital storage media remains accessible and usable for as long as required in accordance with an approved disposal authority.

Principle 5—Preserving Digital Records

State organizations have a strategy to preserve digital records that are required to be preserved for the long-term and to ensure that their file format remains accessible for as long as the records are required in accordance with an approved disposal authority.

Rationale

State organizations have legal responsibilities under the *Freedom of Information Act 1992* and the *State Records Act 2000* to ensure the ongoing maintenance and accessibility of their records. Long-term maintenance is particularly significant for digital records of archival value. Inadequate preservation strategies can render digital records inaccessible and unusable. Allowing digital records to become inaccessible may be considered a breach of the *State Records Act 2000*.

Many records have retention periods greater than one generation of technology. It is important that these records are preserved and accessible for use in daily business using Open Standard, non proprietary formats. Long-term records support strategic planning and decision-making and may be identified as State archives. They act as corporate memory, reducing duplication of work and improving business efficiency.

There may also be evidentiary reasons to keep digital records for extended periods, as part of a risk minimization strategy. Digital records that are inaccessible may expose State organizations to accountability failures and potentially costly consequences, such as legal action.

Minimum Compliance Requirements

State organizations must ensure that:

1. Digital records and their metadata remain accessible and usable for as long as they are required in accordance with an approved disposal authority.
2. For long-term records and archival records, systems planning, design and implementation include provision for conversion or migration of digitized records for the entire life of the record.
3. Strategies for the preservation and maintenance of digital records are developed, implemented and reviewed at regular intervals and staff are aware of and trained in these.
4. A State organization's Recordkeeping Plan contains recovery and restoration procedures for digital records in compliance with SRC Standard 2, Principle 4—Preservation.

Principle 6—Digitization

State organizations ensure that digitized records are as authentic, complete, reliable and usable as the source records from which they are created.

Rationale

Document imaging is the creation of a reproduction or likeness of a document. Where the method of reproduction is based on computers and computer media, document imaging transforms a source document into binary data, a process referred to as *digitization.* A digital reproduction of a source record can be thought of as an electronic reproduction. Whether an electronic reproduction can stand in place of a source record 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 purposes as the source document, then the reproduction will need to be as usable, authentic, complete and as reliable as these purposes require. Reproductions are subject to the same requirements as any other digital record. A State organization must have sufficient confidence in its digitization procedures to certify the authenticity of electronic reproductions.

Where destruction of the source records 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 Plan. Mechanisms and policies used to digitize the record(s) are to be documented in a manner that will allow the use of the digitized record in a court of law and allow the record to be retained and accessible for as long as the record is required.

Minimum Compliance Requirements

State organizations must ensure that—

1. A procedure manual exists that comprehensively describes procedures for digitization, including procedures for security and quality assurance in accordance with SRC Standard 2, Principle 2.
2. Digitization strategies and standards are developed in accordance with accepted best practice standards ensuring the quality of the digitized reproduction.
3. Staff using digitization systems are trained in digitization procedures, and quality assurance mechanisms are established and implemented.
4. Security policy, procedures and guidelines applicable within the organization, as well as digitization specific policies and guidelines, are implemented for digitization systems.
5. Destruction of source records is authorized within the framework of SRC Standard 2, Principle 5 and in accordance with an approved disposal authority.

BIBLIOGRAPHY

Department of the Premier and Cabinet (DPC). (2003) *A Security Management Framework for Online Services.* <http://www.egov.dpc.wa.gov.au/documents/security_management.doc>[Internet] Perth. DPC. [Accessed 25 February, 2008]

National Archives of Australia (NAA). (2004) *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records.* <http://www.naa.gov.au/Images/Digital-recordkeeping-guidelines_tcm2-920.pdf> [Internet] Canberra. NAA. [Accessed 25 February, 2008]

For further information regarding this standard contact
State Records Office of WA
ph: 9427 3360
email: sro@sro.wa.gov.au