Department of **Local Government, Sport and Cultural Industries**
State Records Office of Western Australia

GOVERNMENT OF WESTERN AUSTRALIA

Records Management Advice

Management of Digital Records

An Information Management
Guideline for State Organisations

Version 2.1 – 2024

Contents

GLOSSARY

See the State Records Office - Glossary of Terms, 2024 available on the SRO website.

PURPOSE

The purpose of this guideline is to assist State organisations in ensuring that State records in digital format (e.g. word processed documents, spreadsheets, presentations, databases, email etc) are managed in accordance with SRC Standard 8: *Digital record keeping*.

BACKGROUND

Principle 1 of SRC Standard 8: *Digital record keeping* requires that State organisations ensure that all types of digital records are managed appropriately.

Digital records are an indispensable source of government information which forms part of the State record. They must be integrated into an official record keeping system and managed in accordance with the organisation's record keeping procedures. Digital records should be managed in the same manner as records in other formats. Organisations must therefore ensure that policies and procedures are in place to control the creation, editing, capture, maintenance, storage and authorised disposal of digital records.

To be considered as evidence, a digital record must possess:

- **content** – that which conveys information, for example, the text, data, symbols, numerals, images, sound or vision
- **context** – the background information which enhances understanding of technical and business environments to which the records relate, for example, metadata, application software, logical business models, and the provenance (for example, recipient's name, address, title, link to function or activity, organisation, program or section), and
- **structure** – the appearance and arrangement of the content, for example, the relationships between fields, entities, language, style, fonts, page and paragraph breaks, links and other editorial devices.

SCOPE

This guideline applies to all State organisations as defined in the *State Records Act 2000*.

GUIDELINE

RATIONALE

Organisations must ensure that records created in digital format are managed as State records.

The specific management arrangements developed to implement this guideline may differ amongst organisations depending on information technology environments and operating systems. However, the broad concepts can be applied to any organisation.

1. Policies and Procedures

SRC Standard 2: *Record keeping plans* requires that organisations ensure that record keeping programs are supported by policies and procedures. An organisation should establish policies along with guidelines and procedures for the capture, management and disposal of digital records as State records. Development of policies and procedures should be undertaken in consultation with the organisation's records managers, Chief Information Officers or equivalent officers, information technology personnel, system administrators and users.

Such policies, procedures and guidelines should encompass:

- the legislative and regulatory environment
- the organisation's information and record keeping policy and strategy
- decisions about how and why to capture digital records
- decisions about how long the record is required to be retained and how they may be legally disposed of
- who is responsible for the capture, maintenance, sentencing and disposal of digital records within record keeping systems and user guidelines to support the process
- incorporation of digital records into retention and disposal authorities
- digital records as archives – ensuring the digital records are accessible over time bearing in mind technological changes to hardware and software environments (see SRC Standard 8: *Digital record keeping)*
- security, integrity and authorised access to digital records
- incorporation of record keeping responsibilities in staff education, induction and training programs
- compliance audits.

2. Other Legislation

Organisations should ensure that policies and procedures established for the management of digital records also reflect any legislative requirements specific to, as well as any other legislation affecting, the functions or operations of the organisation.

In addition, legislation, such as the *Electronic Transactions Act 2011* and the *Evidence Act 1906*, which include requirements regarding the admissibility of digital records as evidence must be considered.

3. Registration Responsibilities

All State records have differing values. Some records are needed for ongoing business and some will have ephemeral value only. Ephemeral records do not need to be registered in a record keeping system. All other State records must be captured in the organisation's record keeping system. It is the responsibility of all officers, including temporary staff and contractors to ensure that State records are captured into a record keeping system according to the organisation's approved business rules or policy.

4. Record Keeping Requirements

Digital records, with appropriate metadata, should be captured within the record keeping system to form part of the record of the organisation. This is a minimum requirement to ensure legislative responsibilities, including Freedom of Information, can be met.

4.1 Records should be accessible

Digital records should be accessible to anyone who has sufficient access privileges. That is, authorised staff should be able to access records which are relevant to their role regardless of which business unit or staff member created them.

See also: 4.4 - Records should be readable for the long term

4.2 Records should not be altered

It is important that State records can only be altered in an authorised fashion otherwise they may not be considered reliable evidence. Digital records saved in network directories can be easily altered or deleted. Use of network drives for storage of digital records is **not** appropriate as a management technique. In the event of a dispute about the content of a particular document, the ability to prove that the captured version of the document is identical to the version that was sent or received is paramount. Digital records must be captured in the record keeping system to ensure that the records cannot be altered after dispatch or receipt.

See also: 5. Methods for Capturing and Managing Digital Records.

For evidential purposes it is essential that an access history or log (i.e. metadata) is retained in the record keeping system to indicate who has viewed the record, extracted a copy or modified the content.

4.3 Records should be classified

An important component of records management is classification. That is, records should be classified so that they are linked to and kept in context with other records (paper or electronic) on the same subject. Effective classification facilitates a combined retrieval of a complete picture of events related to a particular business activity, client or project. If related records are not stored together, it decreases their retrievability.

4.4 Records should be readable for the long term

It is highly likely that digital records will be unreadable in as little as five years time due to technological obsolescence unless appropriate actions are taken to ensure their ongoing readability. Irrespective of whether the records are temporary and required to be retained for a short period or of greater value with long term or permanent retention periods, all digital records within current and legacy systems, must be managed appropriately.

Electronic systems must be successfully migrated to ensure viability of the records for the full retention period.

See also:

7.3 Legacy system records

7.4 Migration

SRC Standard 8: *Digital record keeping*.

5. Methods for Capturing and Managing Digital Records

The acceptable methods for the management of digital records are to:

1. capture electronic documents into an electronic document and records management system, and
2. integrate business information systems with record keeping systems or build record keeping functionality into business information systems to ensure that the records are captured and managed appropriately, or
3. where no electronic means of capture is possible, print and file the document.

These methods are not necessarily mutually exclusive and can often be used together. However, the choice of method/s used to manage digital records rests with the organisation.

Use of network drives for storage and management of digital records is **not** appropriate.

5.1 Electronic Document and Records Management System (EDRMS)

The best practice method for managing digital records is to capture them in an EDRMS. An EDRMS provides a user friendly means of capturing digital records at the desktop with minimal effort from the user. These systems allow users to capture electronic documents on to electronic folders (sometimes known as 'virtual' files) and to classify and manage records. The benefits of such a system include:

- improved compliance with record keeping and other business and statutory requirements
- improved processes such as workflow and action tracking
- improved ability to locate and access information
- improved accessibility to digital records in a controlled manner
- protection of sensitive information using security levels, permissions and access controls
- classification and contextual linkage of digital records to paper-based records, and
- improved use of statistical information as metadata can be extracted and manipulated to suit specific business needs.

5.2 Business Information Systems

Business information systems often do not have the functionality, or the required longevity, to manage the records created in the system over time. Many of the transactional business records captured in business information systems are not managed in the organisation's record keeping system. Design specification for business information systems should include record keeping functionality or integration with record keeping systems to ensure that digital records created in those systems are properly managed and accessible for business and legislative requirements.

For further information regarding record keeping functionality in EDRMS and business information systems, refer to the *AS/NZS ISO 16175.1:2021 Information and documentation — Processes and functional requirements for software for*

managing records, Parts 1 & 2.

See also: *Records Management Advice- Records in Business Information Systems*

5.3 Print and file

If the organisation has not implemented the methods described at 5.1 and 5.2, digital records should be printed and filed on the appropriate organisational files. The hard copy document should be registered into the record keeping system as per the organisation's record keeping procedures.

The print and file approach is not appropriate for all types of electronic records (e.g. databases, audio visual files, websites and compound documents). Compound documents are records which contain or have a mixture of attachments in formats such as word processed documents, database segments, email, video, sound recordings and spreadsheets. They may also contain hypertext links to the internet or another network. If electronic records or compound documents cannot be printed, they must be managed and migrated over time, either in an EDRMS or in an electronic environment with appropriate security until they can be disposed of in accordance with an approved records disposal authority.

6. Document Control

6.1 Metadata

Metadata is information associated with electronic records. Record keeping metadata describes the context, management, use, preservation and disposal action of records. Metadata provides contextual information about the record, in a similar way that a file cover provides context to the hard copy record contained in it. For example, it provides information about the date the file was created, who created it, what it's about, when it was closed, a location number etc. As a guideline, the National Archives of Australia (2015) *Australian Government record keeping metadata standard Version 2.2* describes the metadata recommended for capture in record keeping systems.

Many software applications allow for some or all the following metadata (i.e.) document details or properties to be added to a summary screen. For example:

- *title of document
- *subject
- *creator
- *creation and revision dates
- document type
- keywords, and
- *comments/abstract.

NB: * These are considered essential data for complete document metadata.

The completion of profiles or summary information screens when electronic documents are created or saved can greatly enhance their efficient access and retrieval, give meaning and additional context to the record and the way in which it was used within the organisation. Metadata also provides information about the document without having to open the entire document.

See also:

7.2.1 Disposal of metadata

6.2 Retaining drafts

To meet evidential requirements, or to document the development of significant projects or documents, e.g., policies, it is necessary to retain draft documents where alterations provide evidence of a significant change in focus or policy direction. Any drafts that fall into this category should be captured in the record keeping system.

Minor editorial changes such as the correction of spelling or grammatical errors are not regarded as significant alterations. However, where changes to the content or context have occurred, progressive versions (or drafts) must be retained.

Resolution of any uncertainty over what can be destroyed is the responsibility of the Records Manager who should consult with the organisation's Retention and Disposal Authority or contact the State Records Office for further information.

6.3 Copy control

Duplicates or copies of records are an **exact copy** of an original record, where no annotations have been made, and where the **original record** forms part of the organisation's record keeping system. Copies of records that are significantly annotated become an original record in their own right and should be captured into the record keeping system. Duplicates must be identified in the approved Retention and Disposal Authority before disposal can occur.

7. Security and Disposal

7.1 Security

Organisations must establish practices and procedures to ensure digital records are protected from unauthorised access and alteration.

Records should be allocated sensitivity and security ratings and users given particular access rights to protect against unauthorised access and alteration or manipulation.

The following security arrangements should be implemented as a minimum requirement:

- assigning security levels to individuals and folder/file types
- assigning access controls to records, individuals, groups etc
- providing clear security procedures for those using or accessing corporate information from a remote site or from home
- providing guidance for laptop use and security
- establishing strict sanitisation methods for the disposal of equipment
- encouraging staff to lock terminals or to log off when they leave their work stations
- ensuring regular virus checks
- completing regular backups to disk or tape
- establishing quality assurance checks for backup disks or tapes and their storage, and

- protecting all backup medium from contaminants, for example, smoke, food and liquid.

Refer to the Australian Standard *AS ISO 15489 - Records management* for further information on security and access to records.

7.2 Retention and disposal

Under the *State Records Act 2000*, State records may only be destroyed in accordance with an approved records disposal authority.

Records disposal encompasses destruction; transfer to inactive storage; and transfer to permanent or archival storage (online or offline). It is essential to ensure that both short and long term storage of digital records are based on organisational business and legislative requirements. Wherever digital records are stored, they must be managed in a manner which ensures their accessibility, reliability and readability for the entire retention period.

7.2.1 Disposal of metadata in a record keeping or business information system

Following disposal of a temporary record, in accordance with an approved Retention and Disposal Authority, metadata about that record may also be destroyed.

Organisations must ensure they retain sufficient evidence of records that have been disposed of in a disposal list including:

- record/file number if applicable
- title/description
- date range
- Disposal Authority number
- destruction due date

An organisation must assess the risks associated with their functions and determine if there are destroyed temporary records for which metadata should be kept for longer.

Metadata for permanent value records, including State archives, must be kept with that record, and migrated across systems where necessary, indefinitely.

See also: *Records Management Advice - Metadata*

7.3 Legacy system records

Legacy systems must be managed over time to ensure that the records contained within the system are accessible, reliable and readable for as long as required in accordance with an approved Retention and Disposal Authority. If not referenced in a General Retention and Disposal Authority, the required retention period and disposal decisions for all records in legacy systems must be detailed in the organisation's approved Retention and Disposal Authority.

7.4 Migration

Information stored on digital media has a limited life expectancy. This relates both to the life expectancy of the storage medium and the ability of software to read information created using an earlier version or different software.

To ensure access to digital records over time, organisations must provide for the migration of these records across any changes in technology, including developments in EDRMS, business information systems, digital media, software and hardware. This requires the development and implementation of migration strategies which provide for both the periodic transfer of digital records from one storage format to another, and the upgrading of software required to access these records.

The migration process must ensure that the full functionality and integrity of the digital record is preserved, along with any relevant metadata connected with those records, including the establishment of data quality checks. It is advisable for organisations to adopt a collaborative approach between Records and IT departments in all matters concerning the migration of digital records.

The implementation of software upgrades and the conversion of data from one system to another can potentially corrupt records. Therefore, the migration process should be such that the potential for loss of data is minimised. Data conversion should be carefully documented and any alteration, loss of functionality, structure, content or appearance that may occur as a result of the migration process should be documented in the record keeping metadata.

See also: SRC Standard *8: Digital record keeping*.

7.5 Archiving

The management of digital records designated as archives must ensure that those records of permanent value are managed, maintained and successfully migrated to ensure permanent accessibility, reliability and readability. Managing digital archives in this way is distinct from “data archiving” which is a computing term used to describe the periodic transfer of data files offline to backup medium (e.g., magnetic tape) in order to lighten online storage.

Archiving in the record keeping context is a process of maintaining the electronic records permanently (i.e. never to be destroyed), not just for short periods of time.

7.6 Destruction of digital records

Digital records should be destroyed in a way that ensures their complete destruction.

An EDRMS may have a “digital file shredding” option, to enable the destruction of digital records so that they are not recoverable. However, most operating systems do not actually destroy the electronic file when the ‘file delete’ option is selected, they simply remove the name from the directory.

There are several methods to provide greater certainty that data cleansed from digital media and other devices cannot be reconstructed. These methods differ in the manner of application and the level of assurance that data cannot be reconstructed or retrieved. The method chosen should be determined by each organisation dependent upon the risk analysis, conducted prior to disposal, and the

level of sensitivity of the content of the stored data.

The risk analysis should also consider the existence of copies of digital records stored on system backups. Backups are created to facilitate restoration of a system or file in case of accidental or unintentional loss. All organisations should have procedures in place for such systems management. Those procedures should include disposal of the backup disks or tapes after an approved period of time to ensure that copies of digital records are not accessible after the original record has been destroyed.

A complete record of what has been destroyed and under what authority must be kept.

8. Disaster Planning

Dependable backup and recovery procedures protect electronic information from loss and corruption. Information systems should be backed up regularly and recovery procedures tested. The media (servers, disks or tape etc) used to store backed up information should be stored in a safe and secure place.

9. Backlogs of Records

Organisations must develop strategies to address issues relating to backlogs of digital records stored, for example, on network drives, PC hard drives or removable media. Planning should include assigning responsibility for identifying stores of digital records and capturing them into the record keeping system. This is a particularly critical process prior to staff leaving the organisation, or transferring to another department or business unit and when business functions change due to an organisational restructure.

Procedures should be in place to conduct exit interviews with staff leaving the organisation or moving to a different position in the same organisation. The exit interview must include identification of digital records within other repositories and capture of those records within the record keeping system. All digital records in the staff member's control must be reallocated to another staff member or returned to the record keeping system.

10. Training

It is the responsibility of all officers, including temporary staff, contractors and Board members, to ensure that State records are captured into a record keeping system. Management of digital records must be incorporated in an organisation's record keeping training and induction program to ensure that all officers are fully aware of their record keeping responsibilities.

APPENDIX A - Checklist for Implementing the Guideline for Management of Digital Records

Legislative and regulatory requirements with record keeping provisions that apply to the organisation have been identified and documented	
The provisions of the *State Records Act 2000* have been taken into account in the development of digital records management strategies within the organisation	
AS ISO 15489:2002 Records management and *AS/NZS 4360:2004 Risk management* have been considered in the development of digital records management strategies	
A risk assessment has been conducted prior to the development of digital records management strategies	
The Chief Executive supports the digital records management strategy and has ensured sufficient resources for its implementation	
The organisation's broader information and records management plans include digital records management	
Procedures for the creation and capture of digital records that are State records have been developed and implemented	
Information security protocols and procedures have been developed, implemented and maintained to ensure digital records remain inviolate	
Record keeping roles and responsibilities have been identified and documented in digital records management policy and procedures	
All employees and contractors are aware of their responsibilities for creating and capturing full and accurate records of business activity	
The record keeping systems have been designed and implemented in a way that allows the capture of digital records that are State records	
Record keeping metadata is being created and captured along with digital records	
Capture of digital records is monitored and digital records management strategies revised to address areas of risk	
A migration program for captured digital records has been developed and implemented where necessary	
Digital records that relate to the business of the organisation are transferred from network drives (and other systems as appropriate) to the record keeping system as they are developed/finalized	
A strategy for addressing backlogs of digital records (e.g., on network drives) has been developed and implemented where necessary	
A strategy for addressing digital records in legacy systems has been developed and implemented where necessary	
Approved retention and disposal authorities are applied to manage disposal of digital records	
The appropriate level of awareness raising and training for staff creating and receiving digital records has been identified and undertaken	
All staff creating and receiving digital records are aware of and understand the organisation's digital records management policy and procedures	
The use of artificial intelligence in digital record keeping is documented	