Government of Western Australia
Department of Culture and the Arts
State Records Office of Western Australia

State Records Office Guideline

Management of Digital Records

An Information Management Guideline
for State Organizations

Version 2 – January 2015

Contents

GLOSSARY

Aggregation – means any accumulation of record entities at a level above record object (document, digital object), for example, digital file, series.

Archiving - in the recordkeeping context refers to the transfer, management and preservation of records, documents or materials designated as archival records in a separate repository where they are to be held permanently.

Archival record - means a record that is to be preserved permanently (ie never to be destroyed) because of its enduring value (ie. historical, evidential etc.) (also known as a State archive).

Authentic record - means a record that can be proven to:

- be what it purports to be;
- have been created or sent by the person purported to have created or sent it; and
- have been created or sent at the time purported.

Business information system - means:

- An organised collection of hardware, software, supplies, policies, procedures and people, which stores, processes and provides access to an organization's business information; or
- An automated system that creates or manages data about an organization's activities. Includes applications whose primary purpose is to facilitate transactions between an organizational unit and its customers – for example, an e-commerce system, client relationship management system, purpose-built or customised database, finance or human resources systems.

Classification - means the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system.

Digital record - means any record 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. See also: Record.

Disposal - means the process by which records are retained and transferred to the State archive or destroyed. See also: Records disposal authority.

Document - means "*recorded information or object which can be treated as a unit*". (AS/ISO 15489.1 - 2002). For the purposes of this guideline a document is a record.

Duplicate record - means an exact copy of an original record, where no annotations have been made, and where the original record forms part of the organization's recordkeeping system.

Electronic Document and Records Management System (eDRMS) - means an automated system used to manage the creation, use, management and disposal of physical and electronically created documents and records for the purposes of:

- supporting the creation, revision and management of digital documents
- improving an organization's work-flow and
- providing evidence of business activities.

These systems maintain appropriate contextual information (metadata) and links between records to support their value as evidence. eDRMS are a subset of business information systems and recordkeeping systems. Their primary purpose is the capture and management of digital records.

Electronic record - for the purpose of this guideline has the same meaning as digital record.

Ephemeral record - means a record which has only short-term value to the organization with little or no on-going administrative, fiscal, legal, evidential, or historical value. Examples of ephemeral records may include:

- duplicates of circulars (see definition of duplicate);
- duplicate notices of meetings;
- duplicates of minutes and other documents where the original record has already been captured;
- unsolicited advertising material (eg incoming promotional literature, brochures, and leaflets);
- routine or trivial telephone messages; or
- duplicate emails circulated *for information purposes only*.

Ephemeral records may not need to be incorporated into the organization's recordkeeping system. Reference to the organization's policy on ephemeral records should be made in its recordkeeping plan and approved Retention and Disposal Schedule.

Integrity - the integrity of a record refers to its being complete and unaltered.

Legacy system – means an obsolete computer system that may still be in use because its data cannot be changed to newer or standard formats, or its application programs cannot be upgraded.

Long term retention - means the act of retaining records, in an accessible, reliable and readable format for the entire retention period which may mean many decades. In these instances the impact of changing technologies and their effect on the accessibility, reliability and readability of the records must be considered.

Metadata - means data describing context, content and structure of records that must be captured to enable the record to be understood and to support its management and use through time.

Metadata element – means a formally defined term which is used to describe attributes and properties of a record.

Metadata element qualifier – means a mechanism for refining element semantics or to provide information for understanding element values and the terms used.

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

Organization - for the purposes of this guideline means a State organization.

Permanent retention - means the act of retaining the records in perpetuity in an accessible, reliable and readable format. See also: Archival record.

Record - means any record of information however recorded and includes:

- any thing on which there is writing or Braille;
- a map, plan, diagram or graph;
- a drawing, pictorial or graphic work, or photograph;
- any thing on which there are figures, marks, perforations, or symbols, having a meaning for persons qualified to interpret them;
- anything from which images, sounds or writings can be reproduced with or without the aid of anything else; and

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

A record may have any or all of the following attributes:

- information which is of administrative, legal, fiscal, evidential or historical value and is not recorded elsewhere;
- formal communication and/or a transaction between officers (for example, a memorandum, report or submission) or between an officer and another party; or
- documents the rationale behind organization policy, decisions or directives.

Recordkeeping - means the systematic organization and control of recorded information in any format from the time it is created to its final disposition.

Recordkeeping system - means 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.

Records disposal authority - lists categories of records and the retention period, disposal sentence and custody arrangements for each category. State records can only be disposed of under an approved records disposal authority. The State Records Commission approves Records Disposal Authorities.

A records disposal authority may take the form of:

- a general disposal authority (published by the State Records Office);
- a sector disposal authority;
- a retention and disposal schedule;
- an ad hoc disposal schedule; or
- a disposal list.

Reliable record - means a record where the contents can be trusted as a full and accurate representation. See also: Authentic record.

Removable media - means digital storage media which can be removed from its reader device, such as a thumb drive or compact disc, conferring portability on the data it carries.

State archive – see: Archival record.

State archives repository - means the facility which houses archival records under strictly controlled environmental conditions to ensure the longevity of those valuable records.

State organization - is a parliamentary department or a government organization (including local government).

State record - is a parliamentary record or a government record. See also: Record.

State Records Commission (SRC) - is an independent body established under the *State Records Act 2000* (the Act). The SRC's functions include:

- monitoring the operation of, and compliance with, the Act;
- monitoring compliance by government organizations with recordkeeping plans;
- inquiring into breaches or possible breaches of the Act; and
- reporting to Parliament.

PURPOSE

The purpose of this guideline is to assist State organizations in ensuring that State records in digital format (eg word processed documents, spreadsheets, presentations, databases, email etc) are managed in accordance with SRC Standard 8: *Digital recordkeeping*. See also SRO Guideline *Management of email records.*

This guideline aims to provide State organizations with the basis of best practice for the management of digital records.

BACKGROUND

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

State and local government recordkeeping systems must be designed to meet the requirements of efficiency, accountability and the maintenance of State records in accordance with legislative requirements and best practice. Digital records are created within a transactional or business context and provide evidence of that business activity. Electronic documents are typically created and managed using various software applications. An electronic document created or received by an organization is a digital record.

Digital records are an indispensable source of government information which forms part of the State record. They must be integrated into an official recordkeeping system and managed in accordance with the organization's recordkeeping procedures. Digital records should be managed in the same manner as records in other formats. Organizations 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, organization, 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 organizations as defined in the *State Records Act 2000*.

This guideline supersedes:

- State Records Standard 5: *Standard for the management of electronic records in networked computer environments*; and

- State Records Standard 6: *Standard for the management of electronic records in stand-alone computer environments*.

For further information regarding the management of email records see SRO Guideline *Management of email records.*

GUIDELINE

RATIONALE

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

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

See also:

- SRC Standard 8: *Digital recordkeeping;*
- SRO Guideline: *Management of email records;*
- State Records Office Policy 8: *Policy for the ongoing management of electronic records designated as having archival value*; and
- Further relevant guidelines and standards as published by the SRC from time to time.

1. Policies and Procedures

SRC Standard 2: *Recordkeeping plans* requires that organizations ensure that recordkeeping programs are supported by policies and procedures. An organization 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 organization'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 organization's information and recordkeeping 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 recordkeeping 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 recordkeeping* and State Records Office Policy 8: *Policy for the ongoing management of electronic records designated as having archival value*, for more information);
- security, integrity and authorised access to digital records;

- incorporation of recordkeeping responsibilities in staff education, induction and training programs; and
- compliance audits.

2. Other Legislation

Organizations 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 organization.

In addition, legislation, such as the *Electronic Transactions Act 2003* 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 will be needed for ongoing business and some will have ephemeral value only. Ephemeral records do not need to be registered in a recordkeeping system. All other State records must be captured in the organization's recordkeeping system. It is the responsibility of all officers, including temporary staff, contractors and Board members, to ensure that State records are captured into the organization's recordkeeping system according to the organization's approved business rules or policy.

4. Recordkeeping Requirements

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

4.1 Records should be accessible

Digital records should be able to be read by 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 recordkeeping 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 (ie metadata) is retained in the recordkeeping 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 scattered across the organization, it is very difficult to guarantee that all records relevant to a matter have been found.

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;

State Records Office Policy 8: *Policy for the ongoing management of electronic records designated as having archival value*; and

SRC Standard 8: *Digital recordkeeping*.

5. Methods for Capturing and Managing Digital Records

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

1. capture electronic documents in to an electronic document and records management system; and
2. integrate business information systems with recordkeeping systems or build recordkeeping 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 organization.

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 recordkeeping 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 organization's recordkeeping system. Design specification for business information systems should include recordkeeping functionality or integration with recordkeeping systems to ensure that digital records created in those systems are properly managed and accessible for business and legislative requirements.

For further information regarding recordkeeping functionality in eDRMS and business information systems, refer to the *Guidelines for functional requirements for records in business systems* published by the International Council on Archives (2008). (Also published as *AS/NZS ISO 16175 Information and documentation – Principles and functional requirements for records in electronic office environments*).

5.3 Print and file

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

The print and file approach is not appropriate for all types of electronic records (eg 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. Metadata can take the form of indexes, pathways, directory trees, background information attached to emails, word processed documents, databases, signature blocks, header and footer information etc.

Recordkeeping 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 (2008) *Australian Government recordkeeping metadata standard Version 2.0* describes the metadata recommended for capture in recordkeeping systems.

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

- *title of document;
- *subject;
- *author;
- 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 organization. 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, eg 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 recordkeeping 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 organization's Retention and Disposal Schedule 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 organization's recordkeeping system. Copies of records that are significantly annotated become an original record in their own right and should be captured into the recordkeeping system. Duplicates must be identified in the approved Retention and Disposal Schedule before disposal can occur.

7. Security and Disposal

7.1 Security

Organizations 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 sanitization methods for equipment being disposed of;
- 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.

The retention and disposition of digital records should be incorporated into the organization's Retention and Disposal Schedule for approval before destruction or archiving can occur.

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 organizational 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.

It is recommended that disposal is implemented at the file level.

7.2.1 Disposal of metadata in a recordkeeping or business information system

Following disposal of a record, in accordance with an approved disposal authority, metadata about that record must be maintained within the recordkeeping or business information system to demonstrate that accountable processes have been followed.

The following metadata elements and element qualifiers must be retained, as a minimum:

- Record Identifier
- Title
- Creation Date/Time
- Record Relation, where the relationship type is 'documents' (to show the function the record relates to)
- Record Disposal (including all mandatory element qualifiers), and
- Record Event History, where the event type is 'closed' (to show the date the record was closed).

Metadata of destroyed items must be accessible to authorised staff including records managers, Freedom of Information officers and system administrators, however, it is not necessary for that metadata to be routinely presented in search results to general users.

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 records disposal authority. The required retention period and disposal decisions for all records in legacy systems must be detailed in the organization's approved Retention and Disposal Schedule.

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, organizations 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 organizations 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 recordkeeping metadata.

See also:

State Records Office Policy 8: *Policy for the ongoing management of electronic records designated as having archival value*; and SRC Standard 8: *Digital recordkeeping*.

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 (eg magnetic tape) in order to lighten online storage.

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

The State Records Office Policy 8: *Policy for the ongoing management of electronic records designated as having archival value*, provides policy guidelines for the archival management of digital records.

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 organization 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 organizations 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.

Refer also to the State Records Office Guideline: *Sanitizing digital media and devices* for further information.

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. For further information on disaster planning refer to State Records NSW publications *Standard on counter disaster strategies for records and recordkeeping systems* (2002) and Guideline 5: *Counter disaster strategies for records and recordkeeping systems* (2002).

9. Backlogs of Records

Organizations 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 recordkeeping system. This is a particularly critical process prior to staff leaving the organization, or transferring to another department or business unit and when business functions change due to an organizational restructure.

Procedures should be in place to conduct exit interviews with staff leaving the organization, or moving to a different position in the same organization. The exit interview must include identification of digital records within the network drives and capture of those records within the recordkeeping system. All digital records in the staff member's control must be reallocated to another staff member or returned to the recordkeeping 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 recordkeeping system. Management of digital records must be incorporated in an organization's recordkeeping training and induction program to ensure that all officers are fully cognisant of their recordkeeping responsibilities.

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

Legislative and regulatory requirements with recordkeeping provisions that apply to the organization 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 organization	
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 organization'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	
Recordkeeping 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 recordkeeping systems have been designed and implemented in a way that allows the capture of digital records that are State records	
Recordkeeping 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 organization are transferred from network drives (and other systems as appropriate) to the recordkeeping system as they are developed/finalized	
A strategy for addressing backlogs of digital records (eg 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 schedules 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 organization's digital records management policy and procedures	

BIBLIOGRAPHY

International Council on Archives 2008, *Principles and functional requirements for records in electronic office environments – Module 2: guidelines and functional requirements for electronic records management systems,* viewed 13 June 2014, <http://www.adri.gov.au/resources/documents/ICA-M2-ERMS.pdf>.

International Council on Archives 2008, *Principles and functional requirements for records in electronic office environments – Module 3: guidelines and functional requirements for records in business systems,* viewed 13 June 2014. <http://www.adri.gov.au/resources/documents/ICA-M3-BS.pdf >.

National Archives of Australia, *Digital Continuity Principles*, viewed 13 June 2014, <http://www.naa.gov.au/records-management/agency/digital/digital-continuity/principles/index.aspx>

National Archives of Australia 2008, *Australian government recordkeeping metadata standard.* Version 2.0, viewed 13 June 2014, <http://www.naa.gov.au/Images/AGRkMS_Final%20Edit_16%2007%2008_Revised_tcm16-47131.pdf >

Queensland State Archives 2007, *Managing emails that are public records: policy and guideline for Queensland public authorities*, viewed 13 June 2014, <http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/emails_that_are_public_records_policy_and_guideline.pdf>.

Queensland State Archives 2012, *Queensland recordkeeping metadata standard and guidelines*. Version 1.1, viewed 13 June 2014, <http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/QRKMS.pdf>

Queensland State Archives 2009, *Information standard IS40: Recordkeeping.*, viewed 13 June 2014, <http://www.qgcio.qld.gov.au/products/electronic-document-and-records-management/548-qgea/products/qgea-documents/information/2357-recordkeeping-is40>.

Standards Australia International Ltd, *Australian Standard AS ISO 15489 - Records management*. Standards Australia International Ltd, Sydney, 2002.

State Records Authority of New South Wales 2002, *Guideline: Counter disaster strategies for records and recordkeeping systems, viewed 28 August 2014,* <http://www.records.nsw.gov.au/recordkeeping/advice/disaster-management/counter-disaster-strategies-for-records-and-recordkeeping-systems>.