Standard

Managing digital records in systems

Version: 1.0

Date Finalised: 30/11/2020

Date for Review: 30/11/2023

STATE RECORDS
of South Australia

Government of South Australia
State Records

Table of Contents

Standard – Managing digital records in systems

The Standard

Authority

This Standard is issued under section 14(1) of the *State Records Act 1997* (State Records Act).

Agencies must manage digital records in business and records management systems in accordance with the requirements set out in the State Records Act and this Standard.

Scope

This Standard establishes the minimum requirements for managing digital records in business systems.

This Standard also applies to records management systems such as electronic document and records management systems (EDRMS) which are a type of application specifically designed to manage digital (and in some cases physical) records.

In this Standard, 'system' includes a software application, but also the means by which an application is configured and implemented, along with associated procedures.

Executive Summary

The technology environment in which government operates is rapidly transforming how information, including data and records, are created, shared, used and stored. Rarely is information managed in a single centralised system. Agencies therefore need to ensure that all systems used maintain the integrity and reliability of their information assets. This may be achieved through system functionality, integration between systems, migration to another system or through policy and practice.

This Standard:

- Identifies the minimum functional requirements for managing records in systems
- Lists the strategies agencies can adopt to meet the minimum requirements
- Provides a practical checklist for assessing a system against the minimum functional requirements
- Lists optional functional requirements that need to be considered for: migration of records, dedicated records management systems and other general system requirements.

This Standard should be read in conjunction with the *Standard – Minimum recordkeeping metadata requirements*. Other information management standards and guidelines are published on State Records' website.

Business and records management systems should also be established and managed in compliance with the South Australian Protective Security Framework.

Managing digital records in systems

Introduction

Most agencies use business systems to support their work processes and deliver services. While some business systems support general productivity, such as the Microsoft Office suite, other business systems focus on specific business processes, such as case management, work health and safety, or project management.

Many business systems store data and documents. They are often designed to input business information and keep it up to date, potentially overwriting previous data.

The need for a business system to hold the most up-to-date information can compete with the need to record the exact state of the data on which decisions were made at a particular point in time. Loss of historical context can compromise the ability to make assertions about what was known, when and by whom.

Additionally, business systems often do not include the functionality to manage disposal of the data records.

Minimum and additional requirements

Australian and international standards and specifications for managing records in systems already exist. State Records has identified the minimum functional requirements from these industry standards that apply to South Australian government agencies.

State Records endorses use of the international standard *ISO 16175 Processes and Functional Requirements for Software for Managing Records* where an agency requires more detailed specifications than presented here.

The requirements in the industry standards and specifications are designed to be tailored by organisations for their specific business context. Where a requirement in State Records' is different to the industry standard, State Records' standard applies

This Standard assumes that agencies have already analysed the need for evidence of their business and identified which digital information needs to be kept as records. Further assistance with identifying information and records management requirements can be found on State Records' website.

Minimum functional requirements[1]

The following areas of functionality must be in an agency's business or records management system in order to appropriately create and capture, use, manage, and dispose of records.

1. Create and Capture

What is required?	Why is this needed?	Practical considerations
1.1 The system must be able to store digital information required as evidence of business activity as a record.	To ensure there is an authoritative record of business activity.	A record may comprise: » a set of data values in a database that are stored in separate data tables » a comment on an existing record » an email and its attachments or embedded objects » a document » a social media post.
1.2 The system must be able to record details of who created or captured the record and when it was created or captured.	To provide an audit trail for the record's creation and capture.	Metadata required at a minimum should include: » the name of the person » the date information was recorded and/or captured. Details may need to be kept matching system users with names of records creators and their roles in the organisation. Time of capture may be important for some records.
1.3 The system must track any business activity or work processes undertaken within it.	To ensure there is an authoritative record of business activity.	For example, if an application sends an email as part of a work process, the email or its components should be automatically captured as a record of that work process.

[1] This section is a substantial restatement and simplification of requirements outlined in ISO 16175.

1. Create and Capture

What is required?	Why is this needed?	Practical considerations
1.4 The system must be able to separately identify records.	Each record needs to be able to be identified from other records and digital information in the system so agencies can be sure of referencing the appropriate record.	Identification may comprise: » allocating a unique number or identifier to each record » linking an individual record to a folder or other container which has a unique identifier » linking an individual record to a case record which has a unique identifier.
1.5 The system must be able to maintain the structure of individual records and how they are linked to other records.	How the components of a record are linked and how records are presented to a user, affects understanding and integrity of the record. For example, the record approving a property purchase should be linked to the record requesting the purchase.	Maintaining structure may comprise: » storing components separately and linking them e.g. an email and its attachments are stored as separate, linked records » storing components together e.g. an email and its attachments are stored as one record » linking related individual records together in a folder or other container » linking individual records to a case record.

1. Create and Capture

What is required?	Why is this needed?	Practical considerations
1.6 The system must identify the business context of the record, when captured or upon export.	The specific business context can make a great difference to how a record can be understood. The records of one business activity shouldn't be able to be confused with those of another business activity.	Identifying business context may comprise: » including information on screens and in data labels that identify the business process » using categories to tag individual records or case records » using a business classification scheme in an EDRMS. If there are changes to the business context existing records should be linked to their originating business context and not updated with the new business context. If the business context is not identified in the record or its metadata at the time of capture it can be added when the record is exported from the application so meaning is not lost. This can be added as metadata or recorded in external documentation when records are exported.

2. Use

What is required?	Why is this needed?	Practical considerations
2.1 The system must ensure records can be located and read.	To ensure records as evidence of business activity are accessible for business purposes.	Care should be undertaken with use of cloud applications to ensure there is continued access to the records. This can be managed through contractual arrangements and consideration of the need for on premise back up of data.
2.2 The system must be able to apply access restrictions to information content and metadata.	To ensure sensitive records are only accessible to authorised people.	Records should be openly accessible across an agency, unless they contain sensitive information and require access restriction. Access restrictions should be consistent across all information repositories.

2. Use

What is required?	Why is this needed?	Practical considerations
2.3 The system must be able to record details of who accessed, used or edited a record or its metadata.	To provide an audit trail of record access and use.	‘Use’ could include downloading, copying or duplicating, or referencing for others to access, but also direct access or viewing. Metadata required at a minimum should include the time of access or use (this may be important for some records).

3. Manage

What is required?	Why is this needed?	Practical considerations
3.1 The system must be able to apply access permissions to information content and metadata.	To ensure records and metadata are not tampered with, and not altered without authorisation.	System users should not have delete rights, to avoid unauthorised disposal, and may be restricted in their ability to edit or share records. If users need to be able to edit an existing record the system could: » generate a new record » record the changes in the event history of the record (or audit log). ‘Point in time’ reporting which produces a view that reproduces the state of data at a specified date/time may be sufficient to meet this requirement.
3.2 The system must ensure records and their metadata remain accessible and retrievable for minimum retention periods.	To ensure evidence of business activity is available for as long as required.	Records that have been ‘archived’ by the system need to remain accessible, in a readable format. Care will need to be taken to ensure records required to be retained long term, or permanently, remain accessible. Documents saved in file formats that are unsupported or becoming obsolete may become unreadable unless converted to new file formats.

3. Manage		
What is required?	**Why is this needed?**	**Practical considerations**
3.3 The system must record key events in the management of the record, by a user, administrator or the system itself, linked to the record.	To assert the authenticity and integrity of a record it is important to be able to trace actions taken on it during its management (e.g. when it was edited, linked, shared, accessed, exported, etc.). This also allows re-creating records at a particular point in time should this be needed.	Most applications have an audit log. For records management purposes not all actions taken on a record need to be logged. The key events required to be logged depend on the business context, and may be more important for accountable records or high risk business actions. Where possible, audit logs should be designed so they link to specific records rather than maintained in a separate log for all records.
3.4 The system must retain records of key events in the management of the record for as long as required.	The data about the 'state' of a record is essential for maintaining the integrity of the record and meeting accountability requirements.	If an audit log is maintained separately to the records, the entire log will need to be maintained for the required retention period. Where possible, the audit log should be filtered so only key events for records management purposes are retained. The length of time this data is required is determined through disposal schedules.

4. Dispose

What is required?	Why is this needed?	Practical considerations
4.1 The system must ensure records can only be deleted through an authorised process.	Destruction of records is prohibited except in accordance with approved disposal schedules and other disposal determinations under the *State Records Act 1997*.	An authorised disposal process may comprise: » restricting delete permissions to an application administrator, who follows a documented process » linking records to disposal schedules imported into the application » automatically identifying records due for disposal in accordance with a disposal schedule » a workflow that presents records due for disposal for management approval. If the application does not have the required functionality to automate the disposal process this can be undertaken as a manual process and the disposal action and status documented as a record outside of the application.
4.2 The system must keep and be able to migrate records of deletion or export of records.	The disposal process is an accountable process and evidence may be needed of the destruction or export of records.	Records of record deletion or export may comprise: » the specific disposal authority and class authorising disposal » the person authorising disposal » the date disposal was authorised and implemented » what happened to the records, whether deletion or export. If the application does not have the required functionality to document the disposal process this can be undertaken outside of the application.

Other considerations

Many functional requirements in ISO 16175 have not been mandated as minimum requirements for South Australia because they:

- may only be relevant in specific business contexts, such as when migrating records, and could be achieved through use of third party tools
- may only be relevant to the functions of dedicated records management systems such as an EDRMS, rather than applying to all business and records management systems
- are requirements which apply to applications generally, not specifically for records management purposes.

These other considerations are still valuable and could be important for complex or larger enterprise-wide systems.

For migration:

- ability to export records (data and documents) with their metadata, including event history, maintaining their structure and relationships so these can be re-constructed in new applications
- being able to test that essential characteristics of exported records and their metadata have not been changed during export or migration e.g. using checksums, hashes or other mechanisms
- ensuring the new application can import records with their metadata maintaining their structure and relationships
- allowing export to occur more than once, so records should not be automatically deleted upon export
- ability to add metadata during migration.

For records management systems e.g. EDRMS:

- automatically pre-populate metadata (such as from the properties of a document or transmission details from an email)
- enable users to manually enter metadata required for the business
- enable business classification schemes to be updated, maintaining historical classifications where required
- report on creation, usage and disposal of records.

General application considerations:

- authentication of users, including administrators, so only authorised persons can create, edit, access, use and delete records
- enable searching and retrieval of information in the system
- enable information to be duplicated
- enable information to be redacted
- apply access and security controls to data in the system

- apply protective markings to information resources in accordance with South Australian Protective Security Framework policy INFOSEC1: Protecting official information
- keep an audit log of system use and access to data in the system, which may be needed to prove evidence that records have not been tampered with
- report inappropriate logins or access to data, to comply with cyber security requirements
- ensure deleted data and documents cannot be recovered, so information is not inadvertently disclosed.

Strategies for meeting the minimum requirements

Ideally the minimum functional requirements will be designed or implemented within systems, enabling records to be managed digitally and accessible for as long as the record is required.

Software applications may not be able to meet the minimum functional requirements “out of the box”. Instead the requirements will be met through configuration of, or integration between applications, and implementation of procedures, as part of a business system.

Where business systems cannot manage the digital records in accordance with these requirements, agencies must implement strategies to control the records such as:

- using separate applications to manage the records ‘in place’ within the business system (see also Integrating applications)
- implementing manual processes and procedures as part of the broader business system to achieve the same ends
- exporting records and capturing them in a compliant records management system.

Adoption of each of these strategies comes with business risk which should be explicitly accepted prior to implementation of the strategy.

‘Designing’ systems to meet minimum functional requirements

Agencies should ensure that business and records management systems meet the minimum functional requirements in this Standard. This can best be achieved by ‘designing’ systems to meet the requirements through:

- including the minimum functional requirements in application design specifications when preparing tender documents and going to market as part of a procurement process
- using the minimum functional requirements when selecting applications that will store and manage digital records, including cloud based applications
- configuring new and existing systems to meet the minimum functional requirements
- testing new and existing systems against the minimum functional requirements.

This involves being aware of projects to select new systems, or upgrade systems, across your agency.

Assessing existing systems

Some of the minimum requirements set out in this Standard are usually not provided “out of the box” outside of specialised records management systems such as EDRMS.

Typically business systems are not designed to implement the full range of information and records management requirements, especially disposal or export functions. However, there may still be opportunities to configure an existing system to better conform to the minimum functional requirements.

Agencies should assess existing systems against the minimum functional requirements to identify gaps in the functionality of applications and processes, assess the business risks associated with these gaps, and develop plans for mitigating the business risks.

For example, an assessment may reveal that all users can delete all data in an application. Although it may not be possible to import a disposal schedule into the application to automate disposal of records, it may be possible to restrict user deletion rights and implement a manual disposal process for the data, working closely with the business owner and system administrator.

Also, no system lasts forever. A rule of thumb is that many software applications only last about five to seven years. So, even if a business system does not meet requirements now, there may be opportunities in the near future to ‘design’ the next version of the system to meet the minimum functional requirements.

Managing records in business systems that do not meet the minimum functional requirements

In some cases, very little can be done to address the minimum functional requirements in a business system. In this case the only option may be to leave the records in the system and address the issue when the system is decommissioned. This needs to be done with full awareness of the business risks.

Examples of when this might be applicable include:

- records in legacy systems no longer actively used by the agency
- records in unsupported systems nearing end of life
- records only required short term (e.g. less than a few years) where there is low risk if the records become unavailable.

Migration

If records have a retention period longer than seven years, it is likely that they will need to be migrated from one application to another as software or hardware is upgraded, replaced or becomes unsupported. Migration can also be needed during changes to the machinery of government (ie Ministry changes, departmental or agency mergers or divisions).

The migration process requires analysis of both the creating and the receiving applications and must be carefully documented, well tested and any compromises or risks agreed. Because no two applications will be identical, some data will be lost. This needs to be documented and agreed.

Integrating applications

As many applications will not meet the minimum functional requirements “out of the box”, a combination of applications or management systems may be used to meet the minimum functional requirements as an integrated system.

Integration can be implemented in a number of ways depending on the functions of the applications.

- **The record remains in the creating business application and is declared, or notified, to another application.** The second application applies records controls or ‘policies’ such as a business classification scheme or disposal schedule to the record. Event history may also be managed by the second application.
- **A copy of a record is captured from a business application into a records management system**. This is typically how an EDRMS might integrate with general applications such as email applications, where integration between the two applications enables a copy of a record to be moved from one application to the other with minimal effort, enabling a user to link a record to the business context through pre-populated or manually added metadata.
- **A record is moved into a records management systems and a pointer remains.** This is where a business application is responsible for creating the record, but the management of the record is passed to a records management system. Different trigger points can be defined for when the export occurs, but once implemented, the business application holds a pointer, or link, to the records management system which contains the record. This means that the record can be securely managed according to required functionality, while still being accessible to the business application via the link. Variations of this approach can export the records at different defined intervals, for example, end of transaction, end of financial year, or other nominated time period.

Appendix 1: Checklist for assessing a system against the minimum functional requirements

This checklist relates to the Minimum functional requirements table, for use when assessing current or future business or records management systems.

Item	Indicative evidence of compliance	Response
0. Preliminary		
0.1 Is there a clear understanding of what digital information needs to be kept as a record as evidence of business activity, and for how long?	Requirements for evidence of the business activity documented in the system have been identified and documented. Requirements for retention of the information in the business system are included in a current, approved disposal schedule.	
1. Create and Capture		
1.1 Can the system store the digital information required as evidence of business activity, as records?	All required forms of records can be created or captured and stored in the system e.g. emails, social media posts, photos, etc.	
1.2 Can the system record details of who created or captured the record and when?	An audit log is associated with each record and records who created or captured the record and when this occurred.	
1.3 Can the system track any business activity or work processes undertaken within it?	Emails sent or received directly by the system are captured as records in their own right, along with any attachments or embedded objects. Workflow steps are recorded, including any approvals and attachments.	
1.4 Can the system separately identify records?	Each record is uniquely identified via a number, ID, date or other mechanism, either directly or through links to other records or aggregations.	

Item	Indicative evidence of compliance	Response
1.5 Can the system maintain the structure of individual records and link records to other records?	The content and structure of each record is clearly identified, and distinguished from other records. Links exist between related records that are part of the same business activity e.g. all related transactions are identified and/or displayed together.	
1.6 Can the system identify the business context of the record either at capture or upon export?	The business context of each record is clearly identified for example via breadcrumb navigation, or labelling on the screen. The business context can be captured or added as metadata or recorded in external documentation when records are exported from a system.	
2. Use		
2.1 Can the system ensure records can be located and read?	All records in the system are able to be located and read.	
2.2 Can the system apply access restrictions to restrict unauthorised access to information content or metadata?	Content of records cannot be accessed without authorisation. Metadata values cannot be accessed without authorisation.	
2.3 Can the system record details of who accessed, used or edited a record or its metadata?	An event history or audit log is associated with each record and records who accessed, used (eg downloaded, copied) or edited the records and their metadata and when this occurred.	
3. Manage		

Item	Indicative evidence of compliance	Response
3.1 Can the system apply access permissions to information content or metadata?	Users are not given delete rights. Users are not given edit rights, or editing is permitted by users and tracked in event history or audit logs associated with the record.	
3.2 Can the system ensure records and their metadata remain accessible and retrievable for minimum retention periods?	There is a plan for ensuring records and their metadata are maintained in an accessible format for the required retention period.	
3.3 Can the system record key events in the management of the record (by a user administrator or the system itself), linked to the record?	Key events in the management of records have been defined for the specific business activity. An event history or audit log exists for each record, linked to the record, recording defined events.	
3.4 Can the system retain records of key events in the management of the record for as long as required?	Event history or audit logs are kept at least as long as the records. Disposal schedules should indicate the duration required.	
4. Dispose		
4.1 Can the system ensure records are only deleted through an authorised process?	Users are not given delete rights. Administrators only delete data through a formal, authorised process, in accordance with disposal schedules.	
4.2 Can the system keep and migrate records of deletion or export of records?	Evidence exists that records have been deleted or exported and regarding the authorisation for deletion or export.	

Date approved	Approved by	Date for review	Version
30/11/2020	Attorney-General	30/11/2023	1.0

Need further assistance?

Contact
Tel (+61 8) 8204 8791
Email staterecords@sa.gov.au
Web www.archives.sa.gov.au