Digital Preservation

Guideline

Version: 1

Date Finalised: 22/9/2026

STATE RECORDS
of South Australia

Government of South Australia
State Records

Table of Contents

Digital Preservation Guideline

Introduction

Many digital records have retention periods longer than the life of the file format or the system they were created in, and are managed in.

Much like their physical counterparts, digital records deteriorate over time if appropriate measures are not in place. Obsolete file formats, software, and hardware contribute to this deterioration.

This can result in the loss of:

- essential evidence of business activities
- trusted information as a result of alteration
- public access to records documenting rights and legal obligations, and
- digital records destined for the State's archival collection.

Digital preservation is a series of managed activities necessary to ensure continued access to digital records for as long as necessary and beyond the limits of media failure or technological and organisational change.

It involves ongoing monitoring, migration and storage of digital records and, managing the metadata that describes their origin and successive preservation treatment.

Digital preservation safeguards born-digital records and digitised images to ensure they remain accessible and readable in a digital system for as long as required.

Background

The South Australian public sector continues to shift and evolve as new technologies enable more efficiently delivered services. Organisations are now accustomed to managing information digitally by default which comes with new risks to information accessibility, reliability and authenticity.

The value placed on digital records is no different to physical records and many are required to be kept long-term or permanently. As per the Transfer Standard, permanent physical records must be transferred (once administrative use ceases) to State Records custody where the records are stored and preserved in large physical repositories.

Digital records require specialised infrastructure for their preservation. However, despite several attempts State Records of South Australia is yet to secure funding for a solution to centrally store and preserve the State's digital records (also known as a digital archive).

This guideline is not intended to replace a digital archive, rather, highlight and draw agency attention to the real risk of losing long-term temporary and permanent digital records that exists now. The implementation of many of these measures will protect records in active use and those yet to be created. Agencies have a responsibility to begin protecting digital records now and until transfer to the State's central digital archive.

State Records has implemented digital preservation measures for the audio-visual collections in our custody as part of a Deadline 2025 project. There is potential for the digital preservation solution (DPS) to evolve and be expanded to meet the needs of a

digital archive, however, before this can be achieved, additional infrastructure is required.

Purpose and scope

The purpose of this guideline is to establish a set of Digital Record Preservation Principles, strategies and measures to help your agency preserve digital official records. It describes incremental actions and measures, across numerous capabilities, that minimise the risk of losing digital records.

Digital official records determined to be of long-term temporary (where their retention period is 15 years or more) or permanent value require preservation are referred to in this guideline as **digital records**.

Section 3(1) of the *State Records Act 1997* (SR Act) defines 'official records' as information, data and records, in any format (whether digital or hardcopy), where it is created or received through the conduct of government business.

This guideline applies to all digital records in the custody of state and local government agencies and universities that are:

- **born-digital records,** or
- **digitised records**

This guideline **does not discuss preservation digitisation activities**.

Preservation digitisation activities should be performed under the guidance of State Records and in accordance with Australian and international standards. Please refer to the Glossary or contact State Records for further advice on Preservation Digitisation.

This Guideline supports the Information Management Standard issued under section 14 of the SR Act. It should also be read in conjunction with other State Records mandatory standards including the Managing Digital Records in Systems Standard, and Minimum Recordkeeping Metadata Requirements Standard.

Digital Preservation Principles

Adoption of Digital Preservation Principles ensure digital records in the agency's custody remain authentic and accessible in the future through the adoption of the following principles.

Principle 1

Preserve digital records in context, and their content and essential characteristics remain unchanged

- Maintain the integrity of digital records by using business system that comply with digital recordkeeping standards to capture and store digital records and their associated metadata. This provides a foundation for future digital preservation activities.
- Protect original digital records from alteration by providing access via copies or renditions.

Principle 2

Migrate digital records as systems, software and media are upgraded, decommissioned or become obsolete

- Protect digital records against obsolescence by creating, capturing and migrating them to sustainable digital file formats.
- Identify at-risk systems and formats by monitoring them periodically.
- Retain the integrity of digital records (content, essential characteristics and context) through the implementation of migration and digital preservation strategies.
- Migrate digital records to a business system compliant with State Records standards before a system or storage is decommissioned.

Principle 3

Plan and document digital preservation processes

- Prioritise digital preservation resources by implementing a disposal program identifying permanent and long-term value digital records.
- Support consistent digital preservation activities across the agency by documenting digital preservation strategies, quality control and operational procedures.
- Review and monitor digital preservation processes periodically to ensure they continue to address emerging digital formats, technologies, regulations and risks.
- Provide awareness and training to relevant staff on digital preservation measures, including their roles and responsibilities.

Principle 4

Secure and track digital records throughout the preservation process to maintain their authenticity and integrity

- Implement and/or maintain existing access permissions and security measures applied to digital records throughout the preservation process to ensure unauthorised users cannot access or alter digital records and their metadata.
- Keep confidential and sensitive digital records secure by demonstrating an unbroken chain of custody throughout the preservation process.

Digital Preservation Program

Agencies are responsible for ensuring digital records in their custody remain accessible for the minimum retention period, irrespective of changes in technology. When technology changes and/or formats become obsolete, your agency must ensure any affected digital records remain accessible, readable, unaltered and protected. This can be achieved by a digital preservation program.

The risks of digital obsolecence, loss and inaccessibility are not solely resolved by implementing an IT solution. It requires the use of a range of:

- technology (tools, storage and back-up and security),
- resources (business planning, cost modelling, funding, sustainability and skills)
- organisational measures (executive commitment, policy, strategy, procedures, risks and benefits analysis, staffing).

Preparation

Identifying digital records relies on knowing what records you hold and how long they need to be kept for. Your agency can do this by:

- conducting an information asset audit
- assessing their value and risks, and
- sentencing digital records using an approved disposal determination.

State Records Information Governance Guideline provides further advice on these processes. This will also identify digital records at risk of obsolescence and help prioritise those at greater risk than others.

These assessments and audits will highlight both the risk to the records themselves and the risk to the business. Ideally, these risks are included on risk registers that are available and highlighted to agency executives.

State Record's Standards assist agencies establish a sound foundation for preservation activities. Those of particular relevance include the:

- Information Management Standard
- Managing Digital Records in Systems Standard, and
- Minimum Recordkeeping Metadata Requirements Standard.

Digital preservation should be considered during procurement process when digital records are stored in a cloud-based, vendor-managed environment and on software as a service (SaaS) platform.

Roles and responsibilities

Your agency is best placed to determine the governance and accountability arrangements for digital preservation. Ideally it should be a joint responsibility between IM and ICT teams.

Generally, IM staff are responsible for protecting the integrity and accessibility of digital records using digital preservation measures (as currently required with hardcopy

records); ICT administer and provide the systems and storage to support digital preservation.

3.2 Defined Resources, Roles and Responsibilities of the Information Governance Guideline discusses this topic in greater detail.

Assessing your digital preservation maturity

The Digital Preservation Maturity Model (commencing on page 6 of this guideline) will help assess your agency's current preservation status and identify practical goals.

The model is split into three tiers of preservation. These tiers are further dissected into 7 capabilities critical to digital preservation:

- Systems
- Policy
- Migration/decommissioning
- Sentencing and disposal
- Access
- Storage, and
- Incident management.

Any preservation approaches implemented should be reviewed and monitored periodically to ensure it remains relevant to emerging digital formats, technologies, regulation and risks.

Digital preservation strategies

If a digital preservation system is not currently an option, your agency can help protect against obsolescence and functionality loss by manually implementing a range of interim digital preservation measures:

- **Bit preservation** is the process of maintaining digital records in their original format and preserving the bitstreams that form the digital record. It involves storing multiple independent copies across a range of digital storage technologies, regularly checking their integrity (fixity checking), and restoring the digital records if errors are found.
- **Preservation migration** is the process of transferring digital content from one format, system, or storage medium to another using specialist techniques, such as normalisation, to ensure its long-term accessibility and usability.
- **Emulation** involves using current technology to imitate an obsolete system or application in order to access the digital records that it holds.
- **In situ** preservation involves the proactive management of digital records in their original environment (including hardware, software, and operating systems) to maintain its accessibility and functionality over time.

Digital Preservation Maturity Model

The following table outlines three, tiered information management environments an agency may operate within. Each tier lists preservation activities and measures (grouped by seven capabilities; system, policy, migration/decommissioning, sentencing and disposal, access, storage requirements and incident management) that can be implemented as your agency works towards digital preservation. Agencies can be at different tier levels for each capability but should be aiming towards tier 2 and above.

Additionally, agencies may have multiple business systems operating across their environment operating at different tiers. Systems should be assessed and upgraded during their routine upgrade/replacement cycle.

	Tier 1	Tier 2	Tier 3
System	Digital records are saved on network drives, or a business system **not compliant** with State Records Information Management Standards. Digital records: • **Are stored in controlled folder structures** replicating agency classification system in network drives or business systems. • **Folder creation is controlled** by key staff authorised to create folders according to the agency classification system. • **Auditing/tracking metadata** is captured in system or server level audit logs but is limited. It does not meet the auditing metadata requirements under the System and Metadata Standards; there is only partial evidence the record has remained unchanged through its life.	Digital records are captured and stored in a business system **compliant with** State Records Information Management, System and Metadata Standards. This provides a foundation for future complete digital preservation activities by: • capturing and storing digital records ensuring the contextual integrity and reliability of digital records while in active use • capturing the digital records metadata (e.g. descriptive, technical, access, and privacy and rights metadata) • supporting sustainable file formats • generating auditing metadata to maintain the digital records authenticity and integrity • enabling digital records disposal (destruction), and • facilitating the migration of inactive digital records between systems without destroying the record integrity and context. Digital preservation is considered during the procurement process when digital records are stored in a cloud-based, vendor-managed environment and on software as a service (SaaS) platform.	All digital records are ingested from a business system into a commercial digital preservation solution (or an equivalent add-on available for a business system) that uses bit level validation to confirm that digital records remain unchanged over time and format normalisation migration to ensure longevity of record formats. The Digital Preservation Coalition (DPC) provides a list of *Core requirements for a digital preservation system* and *ISO 16363 Audit and Certification of Trustworthy Digital Repositories* provides a benchmark for assessing the trustworthiness of a commercial digital preservation solution. **System requirements** • **Checksums** Record ingest process accepts and stores checksums generated for each record for future fixity/integrity checking. • **Fixity/integrity checking and timestamping** Regular fixity/integrity checking is performed to validate the digital records remain unchanged over time. Timestamping is used as an additional layer of checksum validation. Corrective actions are implemented if bit failure or corruption is detected. • **Metadata** Preservation metadata is generated according to the *PREMIS preservation metadata standard* to record all preservation activities performed on digital records. • **Record destruction** System has record disposal functionality and the ability to capture evidence of record deletion or export. This enables system compliance for storing long-term temporary digital records. **System recommendations** • **Archival information** System must meet the Open Archival Information System (OAIS) framework (ISO 14721), where it is appropriate to the business and function of the agency, allowing interoperability, sharing, harvesting and re-use. • **Preservation migration** System is able to perform format normalisation (preservation migration) into sustainable file formats during record ingest and whilst in storage. The digital record in its original format is also retained.

	Tier 1	Tier 2	Tier 3

Policy	An **Information Management** (IM) policy exists which has been developed in accordance with State Records Standards.
	
	It prohibits staff storing official records in inboxes, hard drives or removable media. Staff are required to save all digital records on central network drives or business systems.
	
	A folder and document titling metadata standard also exists and staff comply with this titling metadata standard.
	
	Agencies understand that digital file formats become obsolete over time and alleviate this by creating digital records in widely used and supported digital file formats (e.g. MS Office formats, pdf.)
	
	• **Informal digital file format policy** (ICT focus rather than IM) exists to assist with limiting the number of file formats used across the agency and is implemented from file creation.
	• **Informal Information asset register exists or is incorporated in ICT Systems Register** is in place. It has an ICT focus rather than IM.
		In addition to an **IM policy**, an **IM Plan** exists which has been developed in accordance with State Records Standards.
		
		A **file format policy** also exists which limits the number and complexity of file formats used across the agency. This helps reduce future format monitoring, maintenance and migration activities. It should also contain the:
		
		• file formats held in business systems
		• the technical characteristics or properties of the file formats (including codecs, colour profiles, encoding, encryption etc.)
		• structure of file formats:
		  ○ standalone
		  ○ multi-part assets (e.g. email containing attachments) or
		  ○ 'containers' with contents.
		• file format migration strategies and rendering capabilities.
		
		The **file format policy** also requires official digital records be created in, or migrated to, best practice **sustainable digital file formats** to protect against degradation or obsolescence during active use and beyond their period of active use.
		
		The **Sustainable Digital File Formats for Creating and Using Records V1.0 April 2020** issued by Council of Australasian Archives and Records Authorities' (CAARA) (of which State Records is a member), lists file formats that it believes have a low risk of becoming unreadable over time. Most of these formats are already in common use and preferred formats for complex file format capture are also provided (eg. websites and social media).
		
		Sustainable digital file formats are:
		
		• **Widely adopted** - widely used and supported around the world.
		• **Unrestricted** – free from patents and legal encumbrance. They preferably use open-source principles.
		• **Well documented** – identity and specifications are publicly available. The specifications are detailed enough that people with the right skills can create software to display it correctly.
		• **Stable** – new versions are released rarely. The format is backwards and forwards compatible or has a clear migration path.
		• **Platform independent** – supported by a wide range of software.
		• **Uncompressed** – if compressed, uses lossless compression (not lossy compression).
		• **Supported** – technical support is readily available from vendors, the community or third parties.
		• **Metadata friendly** – supports metadata.
		Unencrypted - use system and alternative security measures to secure documents.
			In addition to the policies, plans and procedures in the Tier 2 preservation level requirements, a **Digital Preservation Policy** exists supporting key strategies, plans and procedures, detailing the:
			
			• agency's approach to digital preservation
			• essential content and content structural characteristics, and the descriptive, contextual, technical, access/rights, preservation (PREMIS) and management metadata requiring migration.
			• digital preservation strategies adopted for different systems, formats and media
			• programs to monitor and identify any digital records at risk
			• integrity testing required to ensure digital records are not compromised during preservation activities and over time
			• a requirement for each preservation activity to be documented, and
			• references to supporting documents, such as a file formats policy and registry.
			
			Digital preservation is addressed during the procurement process if digital records must be stored in a proprietary format and/or systems to prevent loss if the vendor ceases to support a format or refuses to share the specifications required to preserve it.

	Tier 1	Tier 2	Tier 3
Policy cont.		A **digital formats register** is in place assisting to monitor the range of digital formats used and identify digital records/formats that may require specialised migration/preservation measures. This may be merged with an **Information Asset Register** to ensure all data is updated concurrently, consistent and stored in one location.	
Migration/ Decommissioning	**ICT-based migration and decommission policies** Migration and system decommission is ICT driven focusing on efficiency rather than maintaining the integrity of the digital records. Record integrity risks being lost through its capture or migration. Only some key IM metadata and record characteristics required to maintain record integrity (essential content, content structure, and contextual structure characteristics) are captured or migrated. Some metadata or characteristics may also be altered during the migration process, such as overwriting record creation date or changing a list's bullet structure. Some records are preserved **in-situ** due to lack of skills and resources to migrate records.	**Migration and decommission policies and processes** ensure a digital record's essential characteristics (content and its structure) are retained and the record remains linked to its metadata so record meaning and contextual structure is not lost. Original metadata values are also not changed during migration/decommissioning (e.g. date created, last updated by) **Migration and decommission policies** focus on both ICT and IM migration requirements, including the: • general approach or agency standards • essential content and content structural characteristics, and the descriptive, contextual, technical, access/rights, preservation (PREMIS) and management metadata requiring migration. • approaches for different systems, formats and media • references to supporting documents (e.g. file formats policy and registry) • programs to monitor and identify any digital records at risk, and • post-migration quality control procedures that ensure digital records are not compromised during migration. A **migration plan** is developed for each system/format migration project to document the migration process itself including: the initial analysis, the migration process and testing required, and any agreed risks and compromises required to facilitate the migration. **Emulation or in-situ** preservation measures are implemented where migration measures are not possible or where records have short retention periods.	**Preservation migration policy and projects** ensure digital record's essential characteristics (content and its structure) are retained and the record remains associated with its metadata ensuring record meaning and contextual structure is not lost. Original metadata values are also not changed during digital preservation activities. Preservation migration projects are also capable of: • **integrity/fixity checking** to test the preserved digital record and its metadata have not been changed during digital preservation activities, and • **format normalisation** into sustainable file formats during record ingest and whilst in storage. The use of **emulation or in-situ** preservation measures is kept to a minimum and only used when bit preservation or migration measures are not possible.
Sentencing and Disposal	Digital records are **sentenced when records become inactive** or during system decommissioning. Their preservation value is not known until records are inactive risking loss in the meantime through file corruption and obsolescence. An **ad hoc records disposal program** identifies some digital records. Key digital record series are acknowledged as requiring preservation but no preservation measures are implemented.	Digital records are **classified and ideally sentenced at the time of creation**, at file or aggregate level, using a business classification scheme and a current disposal determination (i.e. disposal schedules). This will ensure their preservation value is known and they can be managed according to their value from record creation and monitored to prevent corruption and obsolescence. A **records disposal program** and **disposal functionality within systems** facilitates identifying digital records and allows the destruction of temporary value records. Digital preservation resources are only directed to some digital records.	An **active records disposal program** identifies digital records allowing the agency to prioritise digital preservation resources. Long-term temporary digital records are destroyed from the digital records preservation system when their retention period ends, in accordance with the agency's records destruction procedures.

	Tier 1	Tier 2	Tier 3
Access	There is **no access and record security policy,** risking unauthorised manipulation of digital records. **Access and record security occurs by closing and restricting access** to files/folders when no longer required for administrative use by**:** • changing personnel access at system level (e.g. to individuals) • changing access rights at system level (e.g. to read only) • applying access restrictions at folder or document level, and • using and maintaining security controls and settings within systems rather than using password protection and encryption.	An **access and record security policy** protects against unauthorised manipulation of digital records. **Access and record security is maintained by closing and restricting access** to files/folders when no longer required for administrative use**:** • changing file/folder access controls within business system, and the type of access rights permitted on inactive files (e.g. to read only) • changing a record's status from active to inactive using business system functionality • using and maintaining security controls and settings within systems rather than using password protection and encryption, and • migrating system/file access controls and security settings across during system/file migrations.	In addition to the access and record security policy in Tier 2 preservation measures, the preservation system **automatically protects** the integrity of preserved digital records and their metadata when accessed. Digital records access controls and security settings are transferred during preservation migration.
Storage	An **IT storage system** exists which may consist of a combination of online storage systems and offline media (e.g. removable storage devices and media, external hard drives etc.) and different types of storage technology however its development and administration is ad hoc posing a high risk to the agency. Storage systems and media is managed and refreshed/migrated on an ad hoc basis at an individual level rather than as an agency strategic IT activity, to address degradation and obsolescence. Some storage may remain unmanaged (such as removable USB storage or external hard drives) resulting in loss of access to digital records through storage media misplacement, degradation and obsolescence.	Systems storing digital records vital to an agency business operations need to observe higher storage standards and more rigorous mitigation processes than general digital storage. A **resilient IT storage system** is used that consists of a combination of online storage systems and offline media, and different types of storage technology. Some systems are held in separate geographic locations to spread risk and enable quick recovery following an ICT disaster incident. Storage systems and media are actively managed and are refreshed/migrated periodically between storage system generations and media to address degradation and obsolescence. Digital records stored on removable storage devices are captured into a compliant business system.	A **resilient IT storage system** is used that is designed specifically to support digital preservation activities. It may consist of: • a combination of online storage systems and offline media • different types of storage technology to spread risk achieving a balance of data safety and manageable cost, and • multiple independent copies of digital records are held in different geographic locations (ideally with different disaster threats levels) to assist with repairing damaged digital records. Preservation IT storage systems and media are actively managed and refreshed/migrated periodically between storage systems and media generations to address degradation and obsolescence.
Incident Mgt.	Ad hoc and/or standard ICT incident and/or disaster recovery backup program is in place.	A standard ICT incident and/or disaster recovery backup program is in place.	A robust digital preservation-focused incident and/or disaster recovery backup program is in place.

Glossary

Term	Definition
Aggregate level	A set, group or accumulation of individual records that are directly related to the same subject, activity or transaction
Bit	The unit of information in computing. Bits are binary (one of two values) and are usually a 1 or a 0. For example, in extended ASCII code the character A is represented by the bits 01000001. For additional context, there are 8 bits in a byte, 1024 bytes in a kilobyte, 1024 kilobytes in a megabyte, and so on.
Bit level validation	The process of checking and verifying the individual bits of a digital record to ensure they have not been altered or corrupted.
Bit preservation	The process of maintaining digital records in their original format and preserving the original bitstreams that form the digital record. It involves storing multiple independent copies of the digital records across a range of digital storage technologies, regularly checking their integrity (fixity checking) and restoring the digital records if errors are found.
Bit stream	A sequence of bits, in a specific order, transmitted or processed in a continuous flow.
Born-digital record	A record created in a digital environment and managed digitally.
Checksum	A unique alphanumerical value calculated using a specific algorithm. It is used to verify the integrity of a digital record – if the value changes, the digital record has been altered.
Content	The information contained within a record (for example, text, numerals, images etc. and all pages).
Content Structure	The appearance and arrangement of the content, e.g. font type and colour, heading styles, bulleting and table structure, page breaks, and dependencies such as hyperlinks. How the record is presented to a user affects the users understanding of the record content and the integrity of the record.
Context	The knowledge necessary to sustain a record's meaning or evidential value. Context describes the 'who, what, where and why' of records creation and management. Contextual information is recorded in metadata. *Keeping Archives 3rd ed*
Contextual Structure	A record's relationships to other records and business activities, and the structure of an individual record's components (eg. email

Term	Definition
	attachments stored separately as linked records or together as one records).
Digital preservation	A series of managed activities necessary to ensure continued access to digital records for as long as necessary and beyond the limits of media failure or technological and organisational change. It involves ongoing monitoring, migration and storage of digital records, and managing the metadata that describes their origin and the successive preservation treatments on the records.
Digital record	This guideline refers to digital records as official records determined to be of long-term temporary (where their retention period is 15 years or more) or permanent value that are born-digital (such as emails, Word documents etc.) or digitised.
Digitised record	A digitally scanned copy of a physical record.
Emulation	The use of current technology to imitate an obsolete system or application in order to access the digital records that it holds.
File	An organised container for records kept together because they relate to a specific subject, activity or transaction.
Fixity	The assurance that a digital file has remained unchanged, i.e. fixed.
Fixity checking also known as **Integrity checking**	The process of ensuring a digital record has not been altered, corrupted or tampered with. There are many methods, including: • checksums • cryptographic hashes • digital signatures, and/or • validation against expected formats. Fixity checking is a process conducted periodically over time, specifically used in digital preservation. Integrity checking can also be applied outside of digital preservation processes, such as general migration.
ICT Incident	An ICT incident is any unplanned interruption to an IT service, or reduction in the quality of an IT service, or associated infrastructure. Also includes cyber security incidents. *Office of the Chief Information Officer (OCIO)*
Ingest	The process of importing a digital record (and its metadata) into a preservation solution while verifying its integrity through fixity checks and format validation.
In situ preservation	The proactive management of digital records in their original environment (including hardware, software, and operating systems) to retain digital record accessibility and functionality over time.

Term	Definition
Long-term temporary value	Records with a retention period of 15 years or more.
Lossless compression	A method of compressing digital records so all file parts are retrievable when decompressed, rendering the file the same. This method limits the amount you can compress a digital record.
Lossy compression	A method of compressing digital records where some information is permanently removed, rendering them irretrievable. This means the file will not be the same when decompressed. This allows you to reduce the size of a file significantly.
Metadata	The details needed to identify, describe, manage and understand records so they act as authoritative evidence of business activity. It includes descriptive metadata (information about the record content itself), contextual metadata (its relationships to other records and business activities), technical metadata (file format, resolution, image size), access and rights metadata (access, use and reuse), preservation metadata (preservation actions – See PREMIS) and management metadata (disposal).
Normalisation	The process of transforming a digital record from one data format (typically proprietary) to a sustainable data format (typically an open standard).
Official Record	The term 'official records' is defined by section 3(1) of the *State Records Act 1997*. It refers to information, data and records, in any format (whether digital or hardcopy), where it is created or received through the conduct of government business. Other State Records policy documents may refer to the term 'information assets' which is also intended to incorporate the definition of official records as defined by section 3(1).
Open Archival Information System (OAIS)	ISO 14721 *Reference Model for an Open Archival Information System (OAIS)* framework is the international standard that describes the components and processes that are required for any trusted repository of digital information, including a digital archive. The OAIS model is made up of six 'functional entities' (ingest, archival storage, data management, administration, preservation planning, and access) that must be in place and interact for a repository to operate.
PREMIS preservation metadata standard	The PREMIS Data Dictionary for Preservation Metadata is the international standard for metadata to support the preservation of digital objects and ensure their long-term usability.

Term	Definition
Preservation digitisation	Preservation digitisation involves creating a digital copy which acts an effective long-term surrogate for fragile paper and other analogue originals, e.g. audio-visual records. It also facilitates the creation of derivative files to meet access requirements (e.g. online access) and minimise the physical wear and tear caused by handling fragile hardcopy records. Once created, digital preservation measures need to be applied to the digital copy files to ensure they remain accessible and usable over time. *National Archives of Australia*
Preservation migration	The process of transferring digital content format, system, or storage medium to another to ensure its long-term accessibility and usability. It involves specialised activities such as normalisation. This transformation is recorded in preservation metadata.
Resilient IT storage system	A resilient IT storage system has multiple 'back-up'/mitigation layers to mitigate the event of one failing and loss of digital records. It consists of storage media contained within a server that provides built in resilience to various failure modes by using inbuilt redundancy and recovery.
Retention period	The minimum period of time for which records should be kept to meet regulatory, business and community requirements. Retention periods and disposal actions (either permanent retention or secure destruction) are documented in disposal determinations (commonly known as Disposal Schedules) approved by State Records Council.
Sentencing	Sentencing is the process of applying retention periods to digital or hardcopy records, at file or aggregate level, from an approved disposal schedule. For digital records it is recommended that sentencing occurs during system design or when the record is created (at file or aggregate level) and can be automated by linking record classification to GDS/RDS classes. Sentencing can also occur as retrospective activity once records are inactive prior to disposal. For digital records this risks the records becoming corrupt or obsolete in the meantime.
Unbroken chain of custody	The continuous, documented, and secure management of digital records from creation or receipt through all stages of their management (including storage, access, migration, and archiving) to ensure their authenticity, integrity, and reliability over time.

For more guidance see also:

What is Digital Preservation?
https://www.dpconline.org/digipres/what-is-digipres

Digital Preservation Coalition's (DPC) Digital Preservation Handbook
https://www.dpconline.org/handbook

DROID (Digital Record Object Identification) supported by *PRONOM*

An automatic digital file format identification tool providing categories of format identification for unknown digital files.

http://www.nationalarchives.gov.uk/information-management/manage-information/preserving-digital-records/droid/

https://www.nationalarchives.gov.uk/PRONOM/Default.aspx

Date approved	Approved by	Version
22/9/2026	Director State Records	1

Need further assistance?
Tel (+61 8) 7322 7077
Web www.archives.sa.gov.au