Department of National Archives

DNA/6 Records Management and Accession Division

Preserving Digital Records

Topic	Preserving Digital Records
Relevant laws	Section 16 (a) & (h) of the National Archives Law No. 48 of 1973
Number	DNA/15/GUIDELINES/2
Effective Date	2025.10.22
Date of amendment	-

CRITICAL REQUIREMENT: Public authorities must consider the following factors **before** procuring or implementing any digital records management system. Consideration of the factors mentioned below at the start itself prevents losses and ensures the chosen system meets requirements of archives and records management.

2. Introduction

2.1 Public authorities are increasingly adopting digital records management systems to improve efficiency and service delivery. These systems include traditional Electronic Document and Records Management Systems (EDRMS) as well as cloud-based platforms such as Microsoft SharePoint, Microsoft 365, Google Workspace, and other similar solutions.

2.2 While implementing these systems, public authorities must ensure compliance with the National Archives Law No. 48 of 1973 and associated regulations. These guidelines outline key requirements to ensure that digital records can be properly preserved, transferred to the National Archives when required, and remain accessible for future generations.

2.3 Before procuring or implementing any digital records management system, public authorities must confirm that the system can meet archival transfer requirements. Public authorities should conduct pilot testing of any new system, including testing export capabilities in required preservation formats, validating metadata capture and retention, verifying retention and disposal automation and demonstrating successful test transfers to the National Archives.

3. Scope and Applicability

3.1 These guidelines applies to all digital records created, received, or maintained by public authorities, regardless of the platform or system used.

3.2 Digital records include but are not limited to:

- Documents (word processing files, PDFs, spreadsheets, presentations)
- Emails and electronic correspondence

- Digital images and scanned documents
- Video recordings (meetings, public hearings, training materials, CCTV footage)
- Audio recordings (proceedings, interviews, oral histories)
- Databases and structured data
- Born-digital records created through automated systems
- Collaborative documents with multiple contributors
- Web content and social media posts

3.3 All systems used for managing digital records must support the requirements outlined in these guidelines, including traditional on-premises EDRMS, cloud-based document management platforms, hybrid systems combining on-premises and cloud storage and custom-developed systems.

4. Technical requirements for digital records management

4.1 All systems must capture and maintain the following minimum metadata for each record:

- Unique identifier
- Title or description
- Creator/author
- Date and time of creation
- Date and time of last modification
- Classification level (public, restricted, confidential, secret)
- Retention period and disposal authority reference
- Related records or file references
- Access restrictions and authorization requirements

4.2 Whether generated from automated systems or not, it is important to accompany digital records with appropriate metadata to provide context and improve searchability. This may involve creating metadata spreadsheets that document the content, structure, and context of the digital records, as well as any other relevant information that may be needed to understand and use the records over time. The naming convention of the digital file must also be carefully considered. Overall, documenting and preserving metadata along with digital records is essential for ensuring their long-term authenticity, reliability, integrity and usability.

4.3 With regard to version control, systems must track all versions of documents throughout their lifecycle, record who made changes and when, preserve version history until final disposition and clearly identify the authoritative or final version. For collaborative documents the complete editing history until the document is finalized should be preserved.

4.4 In connection with search and retrieval, systems must provide full-text search capabilities across all document content, metadata-based search and filtering, advanced search using multiple criteria, export of search results for reporting purposes.

4.5 Systems must implement automated retention schedules based on approved disposal authorities, alert designated officers when records reach the end of retention periods, support legal holds preventing destruction during litigation or investigations, maintain audit trails of all disposal actions, generate certificates of destruction for records lawfully disposed, prevent unauthorized deletion of records before approved disposal dates.

4.6 Systems must provide security features such as encryption of data at rest, encryption of data in transit, prevention of unauthorised copying or downloading, watermarking capabilities for sensitive documents, regular security updates and patch management

4.7 Systems must maintain comprehensive, tamper-proof audit logs recording all access to records (view, download, print), all modifications to records or metadata, all disposal actions, changes to access permissions, system administration activities and failed access attempts. Audit logs must be retained for the same period as the records they document, or longer.

4.8 When using cloud-based systems, public authorities must ensure security certifications, access control and authentication and best practices in vendor management. Public authorities must maintain business continuity with regular backups independent of the cloud provider (at least weekly), tested disaster recovery procedures, exit strategies enabling migration to alternative platforms, documentation of all system configurations and customizations. As far as possible, the 3-2-1 rule (3 copies of data, 2 different media types, 1 off-site copy) should be followed for backups.

5. File Formats for Long-Term Preservation

5.1 Public authorities must ensure their systems can export records in preservation file formats recommended by the National Archives. One common file format used for long-term preservation of digital records is the Tagged Image File Format (TIFF), which is a non-proprietary format that can preserve high-quality images and metadata. However, other file formats such as PDF/A may be used depending on the nature and content of the digital records being transferred. TIFF can contain important metadata.

5.2 This metadata can provide important information about the digital record, such as the creator, date of creation, keywords, and other descriptive information that can help provide context and improve searchability. A digital records management system should be able to generate the required formats for transfer to the National Archives. Public authorities must ensure their systems can export records in a variety of preservation formats including, but not limited to, those listed in the following table:

Type	Recommended Formats	Remarks
Documents	PDF/A-1b, PDF/A-2b, or PDF/A-3b	Preferred for most text documents
Structured documents	XML	
Spreadsheets and data	CSV (Comma-Separated Values) with UTF-8 encoding; PDF/A for final versions with formatting preserved	
Presentations	PDF/A (preferred)	
	ODP (Open Document Presentation)	
Images	TIFF (uncompressed or lossless compression)	For high-quality images requiring preservation of fine detail
Photographs	JPEG 2000 (lossless mode)	
Images with transparency	PNG	

Type	Recommended Formats	Remarks
E-mail	MBOX or EML formats with all attachments	
	PDF/A for individual email messages with attachments embedded	
Video	FFV1 and FLAC codec in Matroska container (.mkv)	Preferred for lossless preservation
Audio	FLAC codec	
Databases	XML export with complete schema documentation	
	CSV export	For tabular data with accompanying data dictionary

5.3 Metadata can accompany file formats in that all file formats must embed or be accompanied by appropriate metadata including creator information, creation and modification dates, keywords and subject classifications, retention and disposal information, and any relevant technical metadata (resolution, colour space, etc.)

5.4 With regard to format migration, public authorities must monitor file format obsolescence, plan for format migration when formats become obsolete, validate migrated files to ensure no loss of content or metadata, document all format migrations in system audit trails.

6. Records Retention and Lawful Disposal

6.1 All digital records created by public authorities must be preserved for a minimum period as specified in records retention and disposal regulations issued under Section 16 of the National Archives Law No. 48 of 1973, and the minimum period specified in Right to Information Act No. 12 of 2016.

6.2 An EDRMS should have automated lawful destruction and transfer protocols built into it. Digital records may only be destroyed if an approved disposal authority issued under the National Archives Law No. 48 of 1973 covers the records, the specified retention period has elapsed, no legal holds or pending investigations require their retention, proper authorization is obtained from designated officers, the disposal is documented in system audit trails.

6.3 When disposing of digital records, it is necessary to use secure deletion methods that prevent recovery, generate and retain certificates of destruction, update system inventories to reflect disposed records, maintain audit trails of disposal actions permanently.

7. Transferring Digital Records to the National Archives

7.1 When transferring digital records to the National Archives, it is important to follow established standards and guidelines for preserving digital records. This includes ensuring that the digital records are in a format that is widely accepted, open, and non-proprietary, and that they are accompanied by appropriate metadata.

7.2 Transfer of digital records to the National Archives is required when records have reached the end of their administrative retention period and are selected for permanent preservation, regulations issued under Section 16 of the National Archives Law No. 48 of 1973 specify transfer requirements, a public authority is being dissolved, records are no longer actively used but have evidential or informational value

7.3 Before transferring digital records, public authorities must ensure records are inactive and are no longer ‘live’ and changing, remove any duplicates or draft versions unless they have independent value, verify that all required metadata is complete and accurate, convert records to approved preservation formats, organise records according to their original filing structure.

7.4 Public authorities must prepare transfer documentation including inventory of records being transferred, metadata spreadsheet with complete information for each record, documentation of any discrepancies between the preservation copy and the original live database, technical documentation of file formats and any special software requirements.

7.5 Public authorities must work closely with National Archives staff throughout the transfer, address any issues or discrepancies identified during quality checks, provide technical support for opening or interpreting records if needed and maintain a copy of transferred records until the National Archives confirms successful receipt and validation.

7.6 After the transfer, public authorities may delete transferred records from operational systems only after receiving written confirmation from the National Archives. Public authorities must refer any access requests for transferred records to the National Archives, which assumes responsibility for long-term preservation and access.

8. These guidelines will be reviewed and updated as needed to reflect technological changes and evolving best practices. Public authorities must report any significant issues or challenges in implementing these requirements to the National Archives.