Standard – Digitizing

Issued By: The Office of the Corporate Chief Information Officer

1. Effective Date

This standard takes effect on July 1, 2018.

2. Application

This standard applies to all government bodies as defined in the *Archives Act.*

3. Context

This standard describes the requirements with which government bodies must comply if their goal is to digitize business records to replace and dispose of master analogue records (original records).

This standard provides direction in the following areas:

- The creation of accurate, reliable, and authentic master digitized records in order to meet legal admissibility requirements;
- The maintenance of accessible master digitized records for as long as required; and
- The appropriate disposal of converted source analogue records after digitization.

This standard supports the Government of the Northwest Territories' (GNWT) *Directive – Digitizing*.

This standard does not apply to digitized convenience copies or archival surrogates.

4. Statement

4.1. Grandfathered programs

Government bodies may continue with any digitization programs in place at the time this standard was issued. It is recommended the government body compare their existing program to this standard. Where there is a difference, the higher specifications should be used.

4.2. Digitization must comply with legislation

Government bodies must determine if there is any legislation that prohibits digitization or requires records to be kept in a particular format or medium. Government bodies must also determine if there are any requirements to maintain authentic and reliable records that may limit the ability to manipulate the master digitized records. Finally, government bodies must determine if there are copyright restrictions to records they did not originate.

Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

4.2.1. Minimum compliance requirement

In order to demonstrate digitization complies with relevant legislation, government bodies must obtain a legal opinion on their digitization program from the Department of Justice or in-house legal counsel.

4.3. Digitization must not expose the government to increased risk

Government bodies must assess the risks of digitizing records and the need to retain the converted source analogue record. Digitization is not recommended where risks are assessed as Major or Extreme. Digitization is also not recommended where risks have a high likelihood of occurring. This may include:

- The authenticity of a record being challenged and the requirement to produce the master analogue record to prove authenticity;
- A master digitized record being incomplete due to poor conversion; and
- A master digitized record being lost due to inadequate records management systems.

4.3.1. Minimum compliance requirement

In order to comply with the requirement to protect the government from risk, government bodies must conduct a risk assessment based on the GNWT's risk matrix.[1]

4.4. Digitization must comply with approved Records Disposition Authorities

Converted source analogue records may only be disposed of if the master digitized record can be classified and scheduled in the Administrative Records Classification System (ARCS) or in an approved Operational Records Classification System (ORCS). If the master digitized records cannot be classified and scheduled in ARCS or ORCS, then the converted source analogue records must not be destroyed.

Early disposition of converted source analogue records must be in compliance with either RDA 2018-02, *Converted Source Analogue Records Schedule*, or in compliance with an existing Records Disposition Authority (RDA), which authorizes the digitization and early disposal of master analogue records.

If the master digitized records have a final disposition of Archival Selection (AS/D) or Full Retention (FR) in an approved RDA (ARCS or ORCS), the government body must submit its

[1] The Program Review Office, Department of Finance, has developed a GNWT risk matrix program for government departments. It can be used to determine overall risk based on an assessment of the likelihood of an event occurring and the impact to the GNWT. Contact the Program Review Office for more information.

Agencies, boards, commissions, and crown corporations may have their own risk assessment tools which may be used in place of the GNWT risk matrix.

Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

digitization plans to the Territorial Archivist for review and acceptance. Converted source analogue records that have a final disposition of AS/D or FR may not be disposed of unless the Territorial Archivist agrees in writing to the early disposal of the converted source analogue records.

New ORCS must identify the secondaries that contain records to be digitized.

When a government body decides to amend existing ORCS for any reason (including to address changes to the records classification structure, changes to retention periods, changes to final disposition, organizational changes or restructuring, or as a result of the five year review of the RDA specified in the Records Scheduling Policy, 6003.00.24), the new version must identify the secondaries that contain records to be digitized, if any.

4.4.1. Minimum compliance requirement

In order to comply with the requirement to schedule master digitized records in an approved Records Disposition Authority, the government body must review its RDAs and determine if the RDA requires amendments. A new RDA may be required to classify and schedule master digitized records.

In order to comply with RDA 2018-02 and any other existing RDAs that authorize the digitization and early disposal of converted source analogue records, the government body must review the RDAs and ensure the requirements of the RDAs have been met by their digitization program.

To ensure compliance with the requirement for archival review and acceptance of the digitization of records designated for Archival Selection or Full Retention, government bodies must submit their digitization plans to the Territorial Archivist for review and approval. This information may be submitted during the review of a new RDA or an amendment to an existing RDA, or it may be submitted as a separate process.

Government bodies must complete the digitization section of the *ORCS Development Guidelines*, 6003.00.25 to comply with the requirements to identify secondaries for digitization in new or amended ORCS.

4.5. Digitization must meet a business need

Government bodies must identify and demonstrate the business need in order to justify and obtain authority for digitizing records. Digitization may occur as either:

- Part of the usual and ordinary course of daily business (business process digitization); or
- Part of a project to digitize a large series of older records (legacy records

Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

digitization).

4.5.1. Minimum compliance requirement

In order to comply with the requirement to demonstrate a business need, government bodies must develop a business case. The business case should be approved by the Director or Regional Superintendent responsible for the program area that has custody and control of the records.

The business case must address:

- The business need for digitization, including how digitization will integrate into existing business processes;
- The risk assessment and any steps to be taken to mitigate the risks;
- Resource requirements, including staff, equipment, software, file size, and storage;
- Methods for quality control and quality assurance, including identifying not only how the quality of the digitized records will be assessed and corrected but also how the effectiveness of the quality control procedures will be measured and improved;
- Requirements for the retention, storage, and disposal of converted source analogue records;
- Technical specifications, including when and where the records will be digitized, who will digitize them, how and in what format the master digitized records will be captured and stored, and how the master digitized records will be managed and maintained for the remainder of their retention period; and
- Outsourcing requirements, if any.

If digitization is planned in support of a government-wide process, initiative, or system, or involves more than one government body, then the leading government body must develop and seek appropriate approval for the business case.

4.6. Digitized records must be stored in a trusted repository

Digitized records, after quality control checks are completed and the digitized records are verified to be the master digitized records, must be stored in a trusted repository capable of safeguarding the authenticity and reliability of the master digitized records. The trusted repository must be able to achieve the following:

- Possession of an established governance framework, including a mission statement and senior management support for its long term use;
- Capture and store commonly used file formats;
- Capture minimum metadata, including title or name, description, subject, file format or type, file size, date created, date modified, name of the creator, name of the

Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

modifier, versions, and file classification numbers;
- Allow authorized users to find and retrieve data based on associated metadata;
- Capable of applying ARCS/ORCS retention and disposition rules to records stored in the repository;
- Impose a disposition hold or halt on materials to prevent disposal of records subject to legal action, an audit, an access to information request, or an investigation;
- Produce an audit trail on the use and modification of stored records;
- A mechanism to log in and authenticate all users; and
- Reside within the information security framework and be protected from unauthorized access and external attacks.

In addition, the government body must ensure they have the following in place to properly manage the records stored in the trusted repository:
- Documented preservation strategies for long term and permanent records;
- Sufficient, long-term financial and human resources;
- Policies and procedures governing the repository's maintenance and use;
- Policies and procedures addressing the preservation of information in the event of technological change or obsolescence;
- Policies and procedures for the reporting of data breaches, corruption, or loss and the steps needed to repair or replace lost or corrupt data in said instances;
- A routine backup schedule that includes all documents and their metadata for disaster recovery purposes and maintain at least one backup in an offsite location;
- A written disaster preparedness and recovery plan;
- A process for staff to test the effect of critical changes to the system;
- A process for staff to prioritize and install new software updates; and
- Assigned, clearly defined roles, responsibilities, and authorities, for employees responsible for the repository, related to implementing changes within the system.

4.6.1. Minimum compliance requirement

In order to comply with the requirement to store master digitized records in a trusted repository, government bodies are required to identify the system that will store the master digitized records, and review the system with the Office of the Chief Information Officer to verify it meets the requirements of a trusted repository.

4.7. Digitization must be documented

Government bodies must create and keep full and accurate documentation of their digitization activities.

4.7.1. Minimum compliance requirement

In order to comply with the requirement to document digitization activities, government bodies must create and keep a procedure manual (set of digitization

Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

procedures) for reference to support the authenticity and reliability of the master digitized records in case of litigation. Government bodies must keep these procedures for as long as the master digitized records are in use.

4.8. Converted source analogue records must be stored and disposed of appropriately

Converted source analogue records may contain highly sensitive information or personal information. All records must be protected against unauthorized access, disclosure, removal, modification, and loss.

It is recommended to store converted source analogue records for an established period of time so they are available to be re-digitized if the digitized record fails quality control checks. The government body must put controls in place to prevent changes to the converted source analogue records.

Once a digitized record has replaced the converted source analogue record as the master record, the digitized record must be treated and used as the master record (master digitized record). No further alterations or additions to the converted source analogue record may be permitted. A converted source analogue record that has been altered following digitization cannot be replaced by the master digitized record and destroyed because the master digitized record is incomplete.

Converted source analogue records must be disposed of in compliance with an approved RDA and the Department of Infrastructure's records disposal procedures.

4.8.1. Minimum compliance requirement

In order to comply with the requirement to ensure the security and confidentiality of the converted source analogue records are maintained, government bodies must develop appropriate security measures. These measures may include procedures for handling and storing the converted source analogue records, screening and training of staff or contractors hired to digitize the records, and providing secure facilities and processes for storing and transporting the records.

In order to protect converted source analogue records from further alteration, government bodies must put procedures or security measures in place to protect the converted source analogue records.

To ensure the appropriate disposal of converted source analogue records, government bodies must consult with the Department of Infrastructure to determine the appropriate disposal mechanism

5. References

Digitizing is subject to a number of provisions, as established by the acts, policies, directives, and standards outlined in Appendix B.

Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

6. Monitoring and Reporting

The Office of the Chief Information Officer will monitor to ensure directives and standards are being followed.

7. Enquiries

All enquiries regarding this standard should be directed to the Department of Infrastructure, Corporate Information Management Division.

8. Approval

This standard is effective from the date approved below.

Corporate Chief Information Officer	Signature	Date
Dave Heffernan		2019-02-01

Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

Appendix A

Definitions

Analogue records refers to physical records of various media types (text, photographic, film, microfilm, blueprints, maps, audio, et cetera) that does not require a computer to view embedded information.

Archival surrogates are digitized copies of archival records held by the NWT Archives produced to facilitate access by the public and to protect original records from handling and damage.

Business process digitization refers to routine digitization of records and the incorporation of the digitized records into business information systems where future actions take place on the master digitized records, rather than on the converted source analogue record.

Convenience copies refers to duplicate copies (either in digital or analog format) of master records created for ease of access and use. Convenience copies are not substitutes or replacements for master records and cannot be relied upon as a record of actions, transactions, or decisions. Convenience copies are typically copied at a lower quality than is required to replace a master record.

Converted source analogue record is a record that has been digitized and is no longer the master record.

Digital is any data or recorded information that exists as binary code (zeros and ones).

Digitization is the process of converting records from analogue (physical) formats to digital formats.

Digitized record is a record that has been converted from an analogue record to a digital record format.

Legacy records refers to an existing set of analogue record that are no longer being added to or modified. They may have been created using filing systems that are either no longer used, or have no apparent organization. They are commonly referred to as backlog records.

Master record is a record that is considered the official record and is considered a true and valid record by both the creator and for legal purposes. Also referred to as a substantive or authoritative record.

Master analogue record is a master record created and manipulated in an analogue (physical) state.

Master digitized record is a record that has been converted from an analogue record to a digital record format, and has met the qualifications (quality control, Records Disposition Authority

Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

approval) to be deemed the master record.

Metadata refers to data describing content, structure, and context of records and their management through time. Metadata can be divided into one of three categories:

- Descriptive metadata describes a resource for purposes such as discovery and identification. Metadata in this area can include such elements as author, title, and description.
- Structural metadata indicates how compound objects are put together. It identifies data format, media format, or the type of data representation and file types, hardware and software needed to render the data, and the compression method and encryption algorithms used, if any.
- Administrative metadata provides information to help manage a resource, such as when and how it was created, and who can access it.

Quality assurance refers to procedures for monitoring and accessing the records system, aiming to maintain a desired level of quality.

Quality control refers to a system of maintaining predetermined standards in a digitized record by testing/reviewing a sample of the output against the specifications within the standard.

Record is a record of information, regardless of its form and characteristics, the means by which it was created and the media on which it may be stored and, without limited the generality of the foregoing, include (a) a document, book, ledger, photograph, image, audio-visual recording, x-ray, map and drawing, and (b) a record created or stored in digital or other intangible form by electronic means, but does not include software or a mechanism that produces records.

Reliable record is a record whose contents can be trusted as being the full and accurate representation of a transaction.

Trusted Repository a trusted repository (secure storage location) provides reliable, long-term access to managed resources to its designated community, now and in the future. A trusted repository for digital assets must protect the authenticity and reliability of the digital assets stored and managed within it.

Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

Appendix B

References

Archives Act sets the legal framework for disposing, transfer, custody and access to records;

Electronic Transactions Act establishes the legal authority of digital records in regards to transactions;

Evidence Act establishes the power and authority of evidence admissible in court, including digital records;

Recorded Information Management Policy (6003.00.18) guides government bodies in the management of their recorded information (regardless of format) and defines the authority and accountability framework;

Records Scheduling Policy (6003.00.24) guides government bodies in the classification, retention, and final disposition of government records;

Management of Electronic Information Policy (6003.00.20) guides government bodies in the management of electronic information;

Electronic Information Security Policy (6003.00.26) guides government bodies in the security of electronic information;

Directive – Digitizing guides government bodies in the development of digitization programs;

Standard – Administrative Records (6003.00.19) establishes a common records disposition authority for administrative records;

Standard – Operational Records (6003.00.32) establishes the standard format for records disposition authorities for operational records;

Guideline – Digitizing provides guidance to assist government bodies in developing and implementing a digitization program;

Guideline – ORCS Development (6003.00.25) provides guidance on the development and formatting of an Operational Records Classification System;

RDA 2018-02 Converted Source Analogue Records provides for the scheduling and disposal of converted source analogue records, when approved by the Territorial Archivist and the Deputy Head;

CAN/CGSB-72.34-2017, Electronic Records as Documentary Evidence is a Canadian national standard for the management of electronic information;

ISO 15489-1:2016, Information and documentation – Records management – Part 1: Concepts and Principles is an international standard for records management programs;

ISO/TR 15801:2009, Document management – Information stored electronically – Recommendations for trustworthiness and reliability is an international standard for the management of electronic information;

ISO 23081-1:2006, Information and documentation – Records management processes – Metadata for records – Part 1: Principles is an international standard for the capture of metadata about records;

ISO 23081-2:2009, Information and documentation – Records management processes –

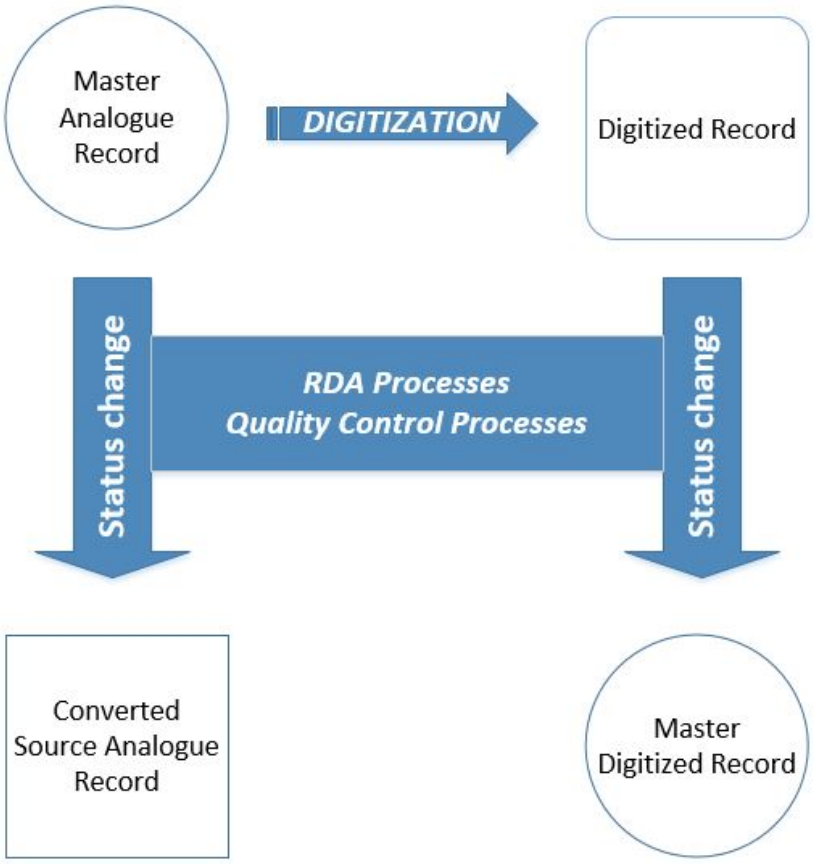
Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

Metadata for records – Part 2: Conceptual and implementation issues is an international standard for the capture of metadata about records;

ANSI/AIIM TR34-1996 Sampling Procedures for Inspection by Attributes of Images in Electronic Image Management (EIM) and Micrographics Systems is a quality control procedure for microfilming and digitizing of records.

Appendix C

Language/Process Map



Approved by CIO - Approval Received 2019-02-01
Document ID 73347259

Appendix D

Revision History

Version	Author	Description
Issue 1 Draft	Digitization Working Group	April 2017-April 2018: Draft prepared for endorsement by the Recorded Information Management Committee and approval by the Informatics Policy Council.
Issue 1 Final	Corporate Information Management, Department of Infrastructure	Final version submitted for approval by Corporate Chief Information Officer.