sport, arts & culture

Department:
Sport, Arts and Culture
REPUBLIC OF SOUTH AFRICA

MANAGING DIGITAL RECORDS IN GOVERNMENTAL BODIES: METADATA REQUIREMENTS

National Archives and Records Service of South Africa

January 2023

National Archives and Records Service of South Africa
Private Bag X236
PRETORIA
0001

Tel.: 012 441 3554

E-mail: Thulisilel@dsac.gov.za

http://www.nationalarchives.gov.za

First Edition, Version 1.1, April 2004
Second edition, April 2006
Third edition, January 2023

Contents

PREFACE

Government bodies' increasing use of electronic systems to conduct their business has significantly changed how records are created and stored. Electronic recordkeeping poses particular challenges to governmental bodies and the National Archives and Records Service, both of which need to ensure that trustworthy records are maintained over time as evidence of official business for accountability, operational continuity, disaster recovery and institutional and social memory. With paper-based records, provided a well-structured file plan is maintained, and the records are physically protected, the evidence they contain remains accessible and readable over time. However, the same cannot be said of digital records in the rapidly changing technological environment.

Governmental bodies need to consider preserving digital records as part of a formal policy of managing records. To promote strategies for the appropriate management of digital records in government, the National Archives and Records Service of South Africa Act (No 43 of 1996, as amended) (NARSSA Act) contains two provisions specifically regarding electronic and digital records systems:

- that the National Archivist shall determine the conditions subject to which electronic records systems shall be managed, and
- the conditions subject to which public records may be electronically reproduced (section 13(2)(b)(ii) and (iii)).

As with other public records, the legislation provides that digital records may not be disposed of without the written authorisation of the National Archivist (section 13(2)(a)). The legislative provisions regarding archival custody take the special needs of digital records into account, in that while public records that have been appraised as having archival value are to be transferred to archival custody after 20 years, the National Archivist may in consultation with the head of a governmental body identify records which should remain in its custody or should be transferred to archival custody at an earlier time (section 11(2)(b)).

Digital records can be defined as records that can be viewed on a computer screen, whether a desktop, laptop, tablet or mobile phone screen. Digital records exist either because a digital version has been made of a paper record or because they were born digital. Born digital records are records that have been natively created in digital format. A digitised record is a record that has been converted from a physical or analogue record to a digital representation. Digitisation is one means of converting an original or source record and is usually carried out through scanning or photographing the source record. For the purposes of this publication, a digital record is an encompassing term referring to digital and electronic records.

The purpose of this document is to guide governmental bodies to assist them in designing metadata schemas as part of their strategic records management policy. Capturing and managing reliable and trustworthy metadata is as important as capturing appropriate content. Without metadata to provide context to individual documents, governmental bodies will not be creating legally admissible records with evidential weight. This document should be read in conjunction with Managing digital records in governmental bodies: Policy, principles and requirements, which contains the broad policies, principles and requirements of the NARSSA Act.

Mr Puleng Kekana

NATIONAL ARCHIVIST

January 2023

1. INTRODUCTION

1.1 General

Records are the output of a governmental body's business and administrative processes. In other words, records are the final proof that a business or administrative process was transacted as essential proof of the business conducted; records should remain unaltered over time for as long as needed. Since one of the National Archives and Records Service of South Africa‘s (NARSSA) responsibilities is to preserve public records with enduring value for use by the public and the state, the NARSSA is not only concerned with the management and accessibility of records over a short period of time. Records created in electronic and paper-based record-keeping systems contain the memory of the decision-making of government and its impact.

The NARSSA is responsible for ensuring that this memory is maintained and protected for centuries to come. To facilitate this, the NARSSA’s role, in terms of the NARSSA Act, is to promote efficient administration by regulating the records management practices of governmental bodies to ensure the sound management of government records. The NARSSA seeks to ensure that governmental bodies capture appropriate metadata to facilitate the long-term accessibility of records in the context of their creation. Metadata ensures the authenticity, reliability, trustworthiness, usability and integrity of records over time for as long as the records are needed. Metadata enables the management and understanding of records. Metadata also needs to be managed to ensure that it is unalterable and thus trustworthy and reliable.

1.2 Benchmark

This document should be read in conjunction with the NARSSA’s publication Managing electronic records in governmental bodies: Policy, principles and requirements. The strategies described in this document are based on the fundamental principle that the management of digital records must be addressed

within the broader context of the policies, standards and practices that deal with managing all forms of recorded information, even though specific types of media may be handled differently. The NARSSA endorses SANS 15489 Information and documentation – Records management – Part 1: General and Part 2: Guidelines as the required benchmarking tool for records management and, in terms of its statutory mandate, requires governmental bodies to put the necessary infrastructure, policies, strategies, procedures and systems in place to ensure that records in all formats are managed in an integrated manner. The NARSSA also recommends compliance with the Minimum Information Security Standard (MISS, 1996) and the Protection of Personal Information Act (Act No 4 of 2013).

The NARSSA also endorses the following standards with a view that they would guide governmental bodies in creating trustworthy, authoritative and reliable records:

- SANS 15801: Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability;
- SANS 17799: Information Technology – Security techniques - Code of Practice for Information Security Management[1]; and
- SANS 23081-1:2006: Information and documentation – Records management processes – Metadata for records – Part 1: Principles.[2] These guidelines were sourced from this standard.
- SANS 18128:2014 : Information and documentation – Risk assessment for records processes and systems
- SANS 18492:2005 : Long-term preservation of electronic document-based information
- SANS 13028:2010 : Information and documentation – Implementation guidelines for the digitisation of records.

[1] This code of practice could be used by governmental bodies that are not subject to the Minimum Information Security Standard (MISS) to guide the design of information security policies and implementations. Governmental bodies that are subject to the MISS should consult with SSA before they use this code.

[2] To obtain copies of all the above-mentioned standards contact the South African Bureau of Standards' Standards Sales Division at: Office address: 1 Dr Lategan Road, Groenkloof, Pretoria;
Postal Address: Private Bag X191, Pretoria, 0001; Telephone: (012) 428-6883; Fax: (012) 4286928; E-mail: sales@sabs.co.za

1.3 **Objective of this publication**

While the NARSSA Act assigns responsibility for determining the conditions subject to which electronic systems should be managed to the National Archivist, the heads of governmental bodies are accountable for implementing the NARSSA's requirements.

This publication aims to guide governmental bodies regarding the minimum metadata required for the long-term preservation of digital records and to assist governmental bodies in designing a metadata schema. Documenting metadata schemas will enable governmental bodies to understand which metadata they need to capture to sustain authentic and reliable records over time. The metadata elements contained in the attached metadata set are considered mandatory to ensure the records' long-term preservation. However, since capturing metadata is also dependent on the business needs of an office and the specific regulatory environment within which the office operates, governmental bodies should add as many other metadata elements as they may find necessary to fulfil their needs.

1.4 Intended audience

The metadata requirements set apply to all governmental bodies, viz. any legislative, executive, judicial or administrative organ of state (including a statutory body) at the national level of government, as well as provincial administrations and local authorities where there is no provincial archival legislation. Once archival legislation is enacted in a specific province, provincial offices and local authorities will receive specific guidelines from the relevant provincial archives service. The guidelines issued by the provincial archives services will not be inconsistent with these guidelines. Should a provincial archive service prefer to continue using these guidelines, the guidelines should be read in conjunction with that province's specific archives and records management legislation.

2. WHAT IS RECORDS MANAGEMENT METADATA AND WHY IS IT IMPORTANT?

2.1 Definition

SANS 15489 Information and Documentation: Records Management – describes the broad records management principles needed to sustain authentic electronic records. It describes metadata as “data describing context, content and structure of records and their management through time”. SANS 23081 Information and documentation – Records Management Processes – Metadata for Records elaborates by saying, “metadata are structured or semi-structured information that enables the creation, registration, classification, access, preservation and disposition of records through time and across access domains. Metadata can be used to identify, authenticate and contextualise records and the people, processes and systems that create, manage, maintain and use them and the policies that govern them.”

Metadata is descriptive data that gives context to electronic documents. **An electronic document cannot be considered a record without the necessary descriptive metadata attached.** Descriptive metadata provides information about where a record comes from, the creator, when it was created, where it is located, etc. Metadata also contains information describing the systems that generated the records and includes information on records management processes and preservation processes such as migration procedures and actions, as well as any other preservation actions taken on records. SANS 23081 also states that “metadata defines the record at its point of capture, or creation and fixes the record into its business context and establishes management control over it. New metadata layers will be added during the existence of the record or its aggregates because of new uses in other business contexts. This means that metadata continues to accrue over time, adding layers of information relating to the context, the records management processes and the business processes in which the records are used. It also adds layers of information relating to structural changes to the record or its appearance”. The capturing of this metadata is

necessary to ensure that authentic and reliable records are sustained for as long as they are required for functional, evidential or historical purposes.

2.2 Benefits of capturing metadata

SANS 23081 identifies the following benefits of capturing metadata[3]:

a) protecting records as evidence and ensuring accessibility, and usability through time;
b) facilitating the ability to understand the records;
c) supporting and ensuring the evidential value of the records;
d) helping to ensure the authenticity, reliability and integrity of the record;
e) supporting and managing access, privacy and rights;
f) supporting efficient retrieval;
g) supporting interoperability strategies by enabling authoritative capture of records created or captured in diverse technical and business environments and their sustainability for as long as required;
h) providing logical links between records and the context of their creation, and maintaining them in a structured, reliable and meaningful way;
i) supporting the identification of the technological environment in which digital records were created and the management of the technological environment in which they are maintained in order that authentic records can be reproduced for as long as they are needed; and
j) supporting efficient and successful migration of records from one environment or computer to another or any other preservation strategy.

[3] SANS 23081 – Information and Documentation – Records management processes – Metadata for records- Part 1: Principles.

3. PRINCIPLES FOR CAPTURING AND MANAGING METADATA

3.1 Roles and responsibilities

Creating and maintaining metadata to sustain authentic records over time requires attention, resources and staff. Capturing metadata is not a once off action. Metadata should be captured at creation and should be updated and maintained as a record moves through its life-cycle and while records management processes are applied to ensure that the record remains authentic evidence of the transactions it relates to.

Specific accountability for the management of metadata should preferably be assigned to the records manager in co-operation with the IT manager. The records manager should be mandated to monitor the creation of metadata and to take corrective actions when required. The reason is that metadata has an accruing nature. Different people are involved in metadata capturing at different stages in a record's life-cycle. It is important that roles and responsibilities regarding metadata capturing and metadata management are defined in the electronic records management policy, to ensure that reliable metadata is captured.

According to SANS 23081[4]:

- Records management professionals are responsible for the reliability, authenticity, usability and integrity of metadata associated with records, and for training users on capturing, managing and using metadata. Records management professionals participate in the definition of metadata requirements, develop related policies and strategies, and monitor the process of metadata creation.
- All employees are responsible and accountable for ensuring the accuracy and completeness of the records management metadata for which they are responsible.
- Executives are responsible for ensuring that internal controls are in place so that clients, auditors, courts, and other authorised users can rely on the information

[4] SANS 23081: Information and documentation – Records management processes – Metadata for records – Part 1: Principles, pp 12-18.

that the organisation produces. Executives are responsible for supporting the use of records management metadata and related policies throughout the organization.

- Information technology personnel are responsible for the reliability, usability and integrity of the systems used to capture and maintain metadata. They are responsible for ensuring that all records management metadata is linked to the related records and that these links are maintained.

3.2 Types of metadata

According to SANS 23081[5] the following types of metadata are important in the records management environment:

a) Metadata about the records. This includes metadata about
   - the identity of the record
     - unique identifier
     - record name
     - record structure
     - data and time of creation
     - relationship with other records
   - the identity of the creator
   - access security restrictions
   - information security classification
   - provenance

b) Metadata about policy, mandates and business rules. This includes metadata about why (policy and mandate) records were created and how (business rules) they were created.

[5] SANS 23081: Information and documentation – Records management processes – Metadata for records – Part 1: Principles, pp 12-18.

c) Metadata about business processes. This includes metadata about the functions and activities that created the records and to which the records relate.

d) Metadata about records management processes. This includes metadata about file plans, disposal authorities and retention periods, as well as about the authorised individuals that were given rights to execute the records management process and the date and time such processes were performed.

3.3 Managing metadata as records

Capturing metadata throughout a record's life-cycle ensures that records can be proven to be authentic and reliable. However, should the metadata be tampered with, the reliability and authenticity of the records it pertains to is affected immediately. Metadata contributes to the "record-ness" of a record. Without metadata to enable understanding of a record in the context of its creation, a record is only a document. Metadata makes a document a record, by fixing it to the context in which it was created.

It is of the utmost importance that metadata should be protected against alterations and tampering like all other records should be protected. It should never be possible to edit system generated metadata. Due to human error, it must be possible for an authorised user, under certain circumstances, to access the user-generated metadata to edit it. This would for example, be required when records were allocated to incorrect folders in the file plan. This delegation to an authorised user should be documented in the electronic records management policy. The policy should also clearly state under which circumstances changes to metadata may be made. To ensure that all changes to metadata are auditable, an audit trail should be captured for all events affecting the metadata.

The metadata repository should be included in the back-up and disaster recovery strategy. It is of no use backing up the records without backing up the metadata. The metadata repository carries the contextual information needed to understand the records, should it be necessary to recover records from back-up media. Without the metadata attached it is impossible to recover authentic records.

The same applies to the migration of metadata. Metadata is also format dependent. It would be of no use to migrate records across hardware and software changes to keep them accessible over time, without doing the same for the metadata. Accessibility would not be of value if the records cannot be understood in context.

3.4 Capturing metadata

Most users rely on metadata to find information but are unaware that it even exists. Governmental bodies should create an awareness of the purpose, creation and usefulness of metadata. The successful implementation of a metadata schema is very dependent on the co-operation of the users.

Not all users understand the benefit of capturing metadata and because they did not have to capture metadata in the paper-based environment, they perceive it to be additional work that they have to do over-and-above the normal workload. It is crucial that users understand that metadata accrues as a record moves through its life-cycle and records management processes and that it may be necessary to capture different pieces of metadata at different stages in a records life-cycle.

Manual capturing of metadata is a very unpopular task and it is recommended that as much metadata as possible should be system generated, based on choice lists, sourced from other sources or inherited from aggregation levels. Inheritance is the principle whereby an object can take on a metadata attribute of its “parent” entity e.g. a record that is filed into a volume or a folder will inherit the metadata of the volume.

The volume, in turn, could inherit its metadata from the folder it is a part of, while the folder could inherit its metadata from the series or sub-series it belongs to, etc.

3.5 Storing metadata

In terms of Section 3(e) of the NARSSA Act, the objects and functions of the National Archives shall be to maintain a National Automated Archival Information Retrieval System (NAAIRS) in which all provincial archives shall participate. In light of this, the NARSSA has implemented the NAAIRS in Access to Memory (AtoM), whereby all entries from the old database have been migrated. NARSSA is also in the process of digitizing some of the archival groups in its custody. Digital records of archival value in governmental bodies, including the metadata, will be ingested into AtoM at the end of the 20-year retention period, however, in terms of Section 11(d), the National Archivist may grant permission for any public records to be transferred to an archives repository before they have been in existence for 20 years. The standards embedded in AtoM are:

- International Standard Archival Authority Record - ISAAR
- General International Standard Archival Description – ISAD (G)
- International Standard for Describing Institutions with Archival Holdings – ISDIAH

NARSSA has ensured that the metadata requirements prescribed to governmental bodies are aligned with the metadata standards used in AtoM to ensure that when digital records are ingested into AtoM, the minimum metadata elements have been captured.

3.6 Designing a metadata schema

Metadata is only of value if all the users understand the usefulness of capturing metadata and if they have a common understanding of the precise meaning and use

of each metadata element. It is therefore necessary to explain the value and use of metadata in a metadata schema. Users should understand that metadata helps a governmental body to:

- meet legal and regulatory requirements by proving authenticity;
- meet records management requirements by providing contextual information and regulating retention and disposal; and
- enable retrieval of records.

A metadata schema is a semantic and logically structured definition of metadata elements. A metadata schema documents the internal relationships between different metadata elements, e.g. the relationship between folders, series and functions in a file plan.

Designing a metadata schema will assist governmental bodies to make a decision about which metadata to capture, to:

- cater for their business needs;
- ensure that they comply with legal and regulatory requirements;
- manage risks inherent in record keeping;
- ensure that in the long term they are able to link records back to the functions that created them.

The schema should also document the rules for managing metadata by documenting:

- responsibilities;
- what metadata to capture;
- where the metadata should be captured from;
- according to what standards the metadata should be captured;
- where to store the metadata;
- how to protect the authenticity of the metadata;
- which laws, policies, and business rules applied to the creation of the records.

Governmental bodies should ensure that they capture the minimum metadata described in this document to enable the long-term preservation of the records and should ensure that they capture as many other metadata elements as are necessary to ensure the continued integrity of the records. The Minimum Mandatory Metadata Elements described in part 4 of this document should be used as the starting point for each governmental body to design and document its own metadata schema.

The Minimum Mandatory Metadata Elements in part 4 contains generic metadata requirements and should not be considered sufficient to replace the need for the design of a metadata schema that is tailor-made to the business requirements of a specific governmental body. The metadata set would only become a proper metadata schema when it is designed to manage risk in a specific implementation.

A metadata schema should

- define the meaning, within a specific office, of the data that should be captured into a metadata field;
- define the choices to be made for those instances where choices are allowed;
- define the source of the data, e.g. whether the data is sourced from:
  - a network log-in, e.g. name of author;
  - from the system e.g. date/time;
  - from authentication systems like a directory access protocol (like LDAP) that contains details about each individual's role, access rights, work units, etc.;
  - from workflow systems for process detail;
  - from e-mail systems for transmission data;
  - from the creating application e.g. application type, date of creation, file name;
  - from a thesaurus;
  - from a template e.g. file reference, document type, etc.

Should metadata be sourced from other systems it is important that the data should be copied to and not only linked to the metadata repository. The rationale behind this is that the information in the source system may be changed, which will cause the

original metadata that was captured for the record to be lost. This is a problem for proving authenticity. It is also a problem if records are transferred into archival custody and the metadata is lost because the source data is not transferred along with the records.

3.7 Metadata registry

Metadata in different systems of the same governmental body is often incomplete and incompatible, causing incomplete information retrieval. It is advisable that governmental bodies give consideration to establishing a metadata registry to enable them to map the metadata in different systems to each other to facilitate automatic translation of metadata elements between systems to achieve interoperability.

Guidelines for establishing and maintaining metadata registries are contained in the ISO 11179 – Information technology - Metadata registries (MDR) series of standards.

4. MINIMUM MANDATORY METADATA ELEMENTS

Note: The attached metadata set covers the whole life-cycle of a record and different parts will be completed by different users at different stages in the record's life-cycle. It covers born-digital records as well as digitized records.

Identity	
Metadata element	Unique identifier*
Indexing Method	System generated
Example	The machine generated indexing number
Purpose and Description	The system ID that uniquely identifies a particular record and distinguishes an object from others in a database.
Responsibility	System administrator ensure proper configuration.
Metadata element	Record title*
Indexing Method	User defined/system generated
Example	Risk management charter

Purpose and Description	• The title of the record given to it by the user. • Must be a sensible name to assist with identification and retrieval. • To be done according to a file naming convention where applicable. • For e-mail messages usually the subject line of the message, however if the subject line is not a sensible description of the content of the message it must be able to be edited in the metadata capturing form.
Responsibility	User
Metadata element	File plan reference number*
Indexing Method	Configure
Example	2/13/3
Purpose and Description	• The numbering convention as it appears in the file plan. • To populate automatically when a subject is chosen from the file plan.
Responsibility	User
Metadata element	Main series description
Indexing Method	Configure
Example	Organisation and control
Purpose and Description	• The main series title as it appears in the file plan. • To populate automatically when lowest level subject is chosen.
Responsibility	Scanning station and/or user
Metadata element	Sub-series description
Indexing Method	Configure
Example	Risk Management
Purpose and Description	• The sub series as it appears in the file plan. • To populate automatically when lowest level subject is chosen. • Repeatable depending on number of levels in the file plan.
Responsibility	Scanning station and/or user

_____

* These are minimum metadata elements that should be retained as a record in the records repository whenever records are destroyed/transferred. Keeping this information as a record, will facilitate compliance with the Promotion of Access to Information Act, 2000 and the Promotion of Administrative Justice Act, 2000.

Metadata element	File plan subject*
Indexing Method	User defined from a pick list
Example	Risk management charter
Purpose and Description	• The formal subject of the folder as it appears in the file plan. • To be picked by the user when creating a record or by the indexer at scanning time.
Responsibility	Scanning station and/or end user
Metadata element	Folder volume/part number*
Indexing Method	Configure
Example	1
Purpose and Description	• The consecutive number of the file/folder part as it appears in the file plan. • The system should only allow filing in open folders and should populate the volume number automatically when a subject is chosen.

Responsibility	System administrator ensures proper configuration
Context	
Metadata element	Author/originator/creator*
Indexing Method	System generated/user defined
Example	MikeT
Purpose and Description	• The intelligent name, rather than login id, of the person or team that is the author of the record. Preferably picked up from the network log-in. • The person by who an e-mail was sent. Preferably picked up from the e-mail transmission data. • The person who signed the paper-based record that was scanned/profiled into the system. This would be a user entry at a scanning station.
Responsibility	• System administrator ensures proper configuration. • Scanning station for information that cannot populate automatically.
Metadata element	Originating organization
Indexing Method	System generated/user defined
Example	Department of Science and Innovation
Purpose and Description	• The name of the specific unit in the organization in which the original record was created. Preferably picked up from the network log in if created internally. • If the record was e-mailed this should preferably be picked up from the transmission data. If not possible it should be user defined. • If received from outside in paper-based format and scanned/indexed into the system it should be user defined at the scanning station at time of indexing.
Responsibility	• System administrator ensures proper configuration. • Scanning station for information that cannot populate automatically.

* These are minimum metadata elements that should be retained as a record in the records repository whenever records are destroyed/transferred. Keeping this information as a record, will facilitate compliance with the Promotion of Access to Information Act, 2000 and the Promotion of Administrative Justice Act, 2000.

Metadata element	Originating sub-office/unit
Indexing Method	System generated/user defined
Example	Risk Management
Purpose and Description	• The name of the specific sub office/directorate/branch in the organization where the record was created. This should preferably be picked up from the network log in. • If the record was e-mailed the information should be picked up from the transmission data. • If received from outside in paper-based format and scanned/indexed into the system it should be captured at time of indexing.
Responsibility	• System administrator ensures proper configuration. • Scanning station for information that cannot populate automatically.

Metadata element	Name of person who declared the record
Indexing Method	System generated
Example	
Purpose and Description	• The intelligent name, rather than login id, of the person that declared the record. • It is the point at which the record came under the full control of the system. • The information is necessary to prove the integrity of a record for admissibility purposes.
Responsibility	System administrator ensures proper configuration.
Metadata element	Addressee
Indexing Method	System generated
Example	
Purpose and Description	• Mandatory for e-mail. Preferably picked up from transmission data. • Optional for other record types. Identifying the person(s) the record was dispatched to.
Responsibility	System administrator ensures proper configuration.
Metadata element	Distribution list/Recipients
Indexing Method	System generated
Example	
Purpose and Description	• Mandatory for e-mail. Preferably picked up from transmission data. • The intelligent names of all recipients of an e-mail message.
Responsibility	System administrator ensures proper configuration.

* These are minimum metadata elements that should be retained as a record in the records repository whenever records are destroyed/transferred. Keeping this information as a record, will facilitate compliance with the Promotion of Access to Information Act, 2000 and the Promotion of Administrative Justice Act, 2000.

Relationships	
Metadata element	Related file/folder
Indexing Method	System generated/User defined
Purpose and Description	• Identifies instances where records have direct relationships to other records, e.g. in a specific business process. • Will assist in managing disposal conflicts, and the provision of information in terms of the Promotion of Access to Information Act, as well as with issues of legal admissibility.
Responsibility	End user
Metadata element	Linkage between record elements
Indexing Method	System generated
Purpose and Description	To enable the linking together of physically separate records or elements that constitute the complete record (for example, an attachment to an e-mail message, an e-form and its data, metadata).
Responsibility	System administrator ensures proper configuration.
Date information	
Metadata element	Creation date

Indexing Method	User defined/system generated
Purpose and Description	• the date that the document was first created prior to being declared as a record or the date of the e-mail sent/received. This should be generated by the system • The date on the paper-based record that was scanned /indexed into the system. • The date format is yyyy-mm-dd.
Responsibility	• System administrator ensures proper configuration. • Scanning station or end user for information that cannot populate automatically.
Metadata element	Date checked in
Indexing Method	System generated
Purpose and Description	• The date the record was checked into the system. • The date format is yyyy-mm-dd.
Responsibility	System administrator ensures proper configuration
Metadata element	Date declared as record
Indexing Method	System generated
Purpose and Description	• The date on which the document was declared as a record and entered into the electronic repository. • It is the point at which the record came under the full control of the system. • The information is necessary to prove the integrity of a record for admissibility purposes. • The date format is yyyy-mm-dd.
Responsibility	System administrator ensures proper configuration

* These are minimum metadata elements that should be retained as a record in the records repository whenever records are destroyed/transferred. Keeping this information as a record, will facilitate compliance with the Promotion of Access to Information Act, 2000 and the Promotion of Administrative Justice Act, 2000.

Metadata element	Folder open/close dates*
Indexing Method	System generated
Purpose and Description	• The date the folder was created (or on which the first record was added) and the date the folder was closed (or on which the last record was added). • The date format is yyyy-mm-dd.
Responsibility	System administrator ensures proper configuration
Metadata element	Part/volume open/close dates*
Indexing Method	System generated
Purpose and Description	• The date the specific part or volume of the folder was created (or on which the first record was added) and the date the part or volume of the folder was closed (or on which the last record was added). • This date will be used to calculate retention periods. • The date format is yyyy-mm-dd.
Responsibility	System administrator ensure proper configuration
Metadata element	Date/time delivered
Indexing Method	System generated
Purpose and Description	• Mandatory for e-mail. • The date and time an e-mail was delivered into another system. • The information is necessary to prove the integrity of a record for admissibility purposes. • The date format is yyyy-mm-dd.

Responsibility	System administrator ensures proper configuration
Metadata element	Date/time received
Indexing Method	System generated
Purpose and Description	• Mandatory for e-mail. • The date and time an e-mail was received. • The information is necessary to prove the integrity of a record for admissibility purposes. • The date format is yyyy-mm-dd.
Responsibility	System administrator ensures proper configuration
Metadata element	Date of last edit
Indexing Method	System generated
Purpose and Description	• Date of last changes made to the document before it was declared a record. • The information is necessary to prove the integrity of a record for admissibility purposes. • The date format is yyyy-mm-dd.
Responsibility	System administrator ensure proper configuration
Metadata element	Record version creation date
Indexing Method	System generated
Purpose and Description	• Creation date of record version in the electronic repository. • The information is necessary to prove the integrity of a record for admissibility purposes. • The date format is yyyy-mm-dd.
Responsibility	System administrator ensures proper configuration

Version control	
Metadata element	Document revision number
Indexing Method	System generated
Purpose and Description	A sequential number for each revision of a document, before it is finalized and declared a record.
Responsibility	System administrator ensures proper configuration
Metadata element	Record version number
Indexing Method	System generated
Purpose and Description	A sequential number for each version of a record kept in the electronic repository.
Responsibility	System administrator ensures proper configuration
Access control	
Metadata element	Access restrictions
Indexing Method	Configure based on policy
Purpose and Description	• Identifying restrictions on access to the record as a whole by indicating permission to user and groups. • Will be inherited from the file plan, and the record type.

Responsibility	• Records manager to define access control on file plan/record type. • Risk manager and security manager to assist the records manager. • System administrator to ensure proper configuration. • User to allocate if not populated automatically.
Metadata element	Access restriction review date
Indexing Method	User defined/or configured beforehand based on a policy
Purpose and Description	The date, preferably annual, on which the access restrictions should be reviewed.
Responsibility	Records manager
Metadata element	Security classification
Indexing Method	User defined/ configured based on policy
Purpose and Description	• Level of security classification, which will have implications for user access restrictions, as indicated by the Minimum Information Security Standard. • Will be inherited from the file plan and record type or set by users.
Responsibility	• Records manager to define access control on file plan/record type. • Risk manager and security manager to assist the records manager. • System administrator to ensure proper configuration. • User to allocate if not populated automatically.

_____

* These are minimum metadata elements that should be retained as a record in the records repository whenever records are destroyed/transferred. Keeping this information as a record, will facilitate compliance with the Promotion of Access to Information Act, 2000 and the Promotion of Administrative Justice Act, 2000.

Metadata element	Sensitivity review date
Indexing Method	User defined/or configured beforehand based on a policy
Purpose and Description	The date at, or time period after, which a review of the security classification is appropriate.
Responsibility	• Records manager to define access control on file plan/record type. • Risk manager and security manager to assist the records manager. • System administrator to ensure proper configuration. • User to allocate if not populated automatically.
Disposal control	
Metadata element	Disposal instruction
Indexing Method	Configured
Purpose and Description	• The action to be taken at the end of the life cycle of the record, e.g. destroy/delete or keep permanently. • Inherited from the specific record type and the disposal schedule. • Based on written disposal authority issued by National Archives and Records Service.
Responsibility	• Records manager defines on file plan and record type. • System administrator ensures proper configuration.

Metadata element	Retention period
Indexing Method	Configured
Purpose and Description	• The standard period of time for which records should be retained before the disposal action is carried out. • Inherited from the specific record type and the disposal schedule.
Responsibility	• Records manager defines on file plan and record type. • System administrator ensures proper configuration.
Metadata element	Disposal authority number*
Indexing Method	Configured
Purpose and Description	• The unique disposal authority number issued by the National/Provincial Archives that authorises the action to be taken against the record. • Inherited from the specific record type and the disposal schedule.
Responsibility	• Records manager defines on file plan and record type. • System administrator ensures proper configuration.

* These are minimum metadata elements that should be retained as a record in the records repository whenever records are destroyed/transferred. Keeping this information as a record, will facilitate compliance with the Promotion of Access to Information Act, 2000 and the Promotion of Administrative Justice Act, 2000.

Metadata element	Disposal action review date
Indexing Method	User defined/system generated
Purpose and Description	• The date on which the scheduled disposal action was reviewed. • The date format is ccyy-mm-dd.
Responsibility	Records manager
Metadata element	Disposal action review comments
Indexing Method	User defined/ configured based on policy
Purpose and Description	A textual description indication why the disposal action was reviewed and what decision has been taken against the record.
Responsibility	Records manager
Metadata element	Destruction/ transfer date*
Indexing Method	System generated
Purpose and Description	• The date on which the records were destroyed/transferred. • The date format is ccyy-mm-dd.
Responsibility	System administrator ensures proper configuration.
Metadata element	Identity of person authorizing the review/destruction/ transfer*
Indexing Method	System generated
Purpose and Description	The intelligent name, rather than login id, of the person that authorized the review of the disposal instruction of the records and/or who authorized the destruction/deletion/transfer of the records.
Responsibility	System administrator ensures proper configuration.
Metadata element	Transfer location
Indexing Method	User defined/system generated

Purpose and Description	A textual description of the location the records were transferred to.
Responsibility	System administrator ensures proper configuration
Record type	
Metadata element	Record type
Indexing Method	User defined from a pick list/built into templates
Purpose and Description	• A description identifying the logical document/record types – e.g. report, memo, letter, which may be a useful aid to identification or processing choices, and which is used as a disposal mechanism. • When not inherited from a document template, the user should define from a pick list.
Responsibility	• Records manager defines types. • System administrator ensures proper configuration.

Presentation and medium	
Metadata element	Storage medium
Indexing Method	System generated
Purpose and Description	Indicates the medium on which a record is kept e.g. paper, CD, magnetic tape, etc.
Responsibility	• Records manager defines medium. • System administrator ensures proper configuration.
Metadata element	Format
Indexing Method	System generated
Purpose and Description	The physical application format type/file e.g. the 3-letter file type, such as .doc, .ppt, .gif, .msg, used in a Windows environment.
Responsibility	System administrator ensures proper configuration.
Metadata element	Presentation format
Indexing Method	System generated
Purpose and Description	Linking between versions where the same record is held in different formats for preservation and for viewing, or where sensitivity editing has resulted in creation of a variant version.
Responsibility	System administrator ensures proper configuration.
Metadata element	Language
Indexing Method	User defined/ configured to pick up from template
Purpose and Description	Identify the language the records was created in to enable retrieval, and linking to translations that might exist.
Responsibility	System administrator ensures proper configuration.
Location information	
Metadata element	Physical location
Indexing Method	Default from file plan

Purpose and Description	• Physical storage location of the paper-based file and its contents. • Also the location of electronic records within a hierarchical storage management system.
Responsibility	Records manager to define. System administrator ensures proper configuration.
Metadata element	Barcode (paper)
Indexing Method	System generated
Purpose and Description	Identifying label for paper files, or the paper or hard copy element of hybrid assemblies, only.
Responsibility	System administrator ensures proper configuration.

System information	
Metadata element	Technical platform
Indexing Method	System generated
Purpose and Description	Information regarding the platform application and format on which the records were generated.
Responsibility	System administrator ensures proper configuration.
Vital record information	
Metadata element	Vital record indicator
Indexing Method	User defined/ configured beforehand based on a policy
Purpose and Description	An indication if the records: • protect the enduring civil, legal, financial, property and other rights of the citizens of a country. These records may never be destroyed. • are needed to continue operational responsibilities under disaster conditions. Office is to decide how many years' worth of records are needed to continue operating in disaster conditions – this will influence the retention period. • protect the legal and financial rights of the governmental body. Office is to decide how many years' worth of records are needed to continue operating in disaster conditions – this will influence the retention period.
Responsibility	• Records manager defines which qualify. • System administrator ensures proper configuration.
Metadata element	Vital record review date
Indexing Method	User defined/ configured beforehand based on a policy
Purpose and Description	The date at, or time period after, which a review of the vital record status is appropriate.
Responsibility	• Records manager defines beforehand. • System administrator ensures proper configuration.
Audit information	
Metadata element	Audit trail

Indexing Method	System generated
Purpose and Description	Identification of users who have taken significant actions on the record through its lifecycle, the action taken (for example: create, edit, copy to new version, delete/transfer, etc.), the date the action was taken.
Responsibility	• Records manager and risk manager define beforehand. • System administrator ensures proper configuration.