Republic of Zambia
Office of the President
Electronic Government Division

PUBLIC SERVICE INFORMATION COMMUNICATION TECHNOLOGY STANDARDS

ELECTRONIC RECORDS AND DATA MANAGEMENT GUIDELINE

Version: 1.0

Published Date: 2023

Document History:

Validation and Distribution

	Name	Issue date
Issued by	The Electronic Government Division	2023
Verified by	Standards Task Team	December 2023
Approved by	National Coordinator	December 2023

Distribution List	
1	Cabinet Office
2	All Public Bodies
3	Online publishing (SZI Website)

Document Revision History:

Version	Date	Author	Remarks
1.0	2023	Standards and Compliance Department	Creation of Documents

Foreword

The Electronic Government Division, SMART Zambia Institute is responsible for formulating and enforcing Information and Communication Technologies (ICT) standards and guidelines across all Public Bodies to facilitate the transition into a Digital Society. In line with its mandate, the e-Government Division has developed Electronic Records and Data Management Guidelines.

As we march forward into the digital era, the Electronic Government Division takes great pride in spearheading the formulation and enforcement of ICT standards across all Public Bodies. Our ultimate vision is to facilitate a seamless transition into a Digital Society, where efficient and transparent governance is a reality for all.

These guidelines represent a fundamental step towards establishing a robust framework for managing records and data, whether in electronic or other formats, throughout the public bodies.

The implementation of this standard will be monitored and enforced by the e-Government Division. Annual audits shall be carried out in public bodies to determine their level of compliance to this standard. The e-Government Division shall issue a certificate of compliance to a public body upon completion of a successful audit assessment. For a non-compliant public body, appropriate action shall be undertaken depending on the extent of the deviation from set standards.

All public bodies are required to ensure full compliance to the Electronic Records and Data Management Guideline for effective and efficient public service delivery.

Percy Chinyama (Mr.)
National Coordinator
Electronic Government Division

Acknowledgment

The successful development of this guideline marks a significant milestone in advancing our government's commitment for efficient and secure electronic records and data management practices. It not only streamlines our operations but also reinforces our dedication to transparency, accountability, and service excellence to the public service.

The extensive work and collaboration demonstrated by the Task Team and the Heads of ICT has been truly impressive. The comprehensive nature of the guideline is a testament to their expertise, dedication, and professionalism. I am confident that this well-structured framework will serve as a valuable resource for Public Bodies in effectively managing electronic records and data. This will ensure the confidentiality and integrity of sensitive information while promoting seamless accessibility.

Moreover, I would like to extend my appreciation for the seamless coordination between all stakeholders involved in this initiative. It is evident that the collective commitment has resulted in a guideline that aligns with international best practices and meets the specific needs of our Government.

On behalf of the Electronic Government Division, I wish to express my sincere gratitude to the e-Government Standards Task Team for their unwavering dedication to the development of this standard. Their expertise, tireless efforts, and visionary leadership have been instrumental in the development of this standard. The division is also indebted to the Heads of ICT in public bodies and stakeholders, whose guidance and commitment have propelled this initiative forward. This document will ensure Standardisation of critical data elements providing seamless exchange of information in Public Bodies.

Musenge

Kasali Musenge (Ms.)
Director Standards and Compliance
Electronic Government Division

Table of Contents

Abbreviations

BCP	Business Continuity Plan
DRP	Disaster Recovery Plan
ERDM(S)	Electronic Records and Data Management, System
ICT	Information and Communication Technology
ISO	International Standards Organisation
ITU	International Telecommunications Union
Public Bodies	Ministries, Provinces and Public Bodies
PDF	Portable Document Format
PDF/A	Portable Document Format Archive
SSL	Secure Sockets Layer
VPN	Virtual Private Network
ZABS	Zambia Bureau of Standards
ZMVA	Zambia Minimal Viable Architecture

Working Definitions

Access Right: The permissions that are granted to a user, or to an application, to read, write and erase files in the computer.

Content: Basic data or information carried in a record; substance of the record that captures sufficient information to provide evidence of a business transaction.

Conversion: Process of changing records from one format to another.

Destruction: It is the process of eliminating or deleting a record, beyond any possible reconstruction. In this guideline, term destruction will refer to a disposal process whereby digital records, record plan entities and their metadata are permanently removed, erased or obliterated as authorised and approved by a disposition authority schedule.

Disposition: Range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments.

Electronic Documents: (Electronic documents are a subset of electronic records.) They are collections of data, which may be produced in the following ways:

i. Original output either created as a text document, small database, spreadsheet, or graphics,
ii. A combination of existing data which may be extracted from databases, text files, e-mail, etc.
iii. Data received from outside the organisation (i.e. Via e-mail, scanning).

Electronic Records: Records that are in machine-readable form. Electronic records may be any combination of text, data, graphics, images, video or audio information that is created, maintained, modified or transmitted in digital form by a computer or related system.

Electronic Records and Data Management System: An automated system used to manage the creation, use, maintenance and disposal of electronic records. An E-records and management system should be able to maintain data and a record along with its associated metadata.

Export: This is a disposition process, whereby copies of a digital record or a group of records are passed with their metadata from one system to another system; either within or beyond the organisation. Export does not involve removing records from the first system.

Long Term: A period greater than ten years.

Metadata: Metadata is data about data. It is data describing the context, content and structure of records and their management through time. Metadata are captured along with electronic records to enable them to be understood and verified.

Migration: It is the act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability.

Record: Information created, received and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in the transaction of business.

Public Service Records and Data Management Technical Committee: A group responsible for reviewing and approving data and records retention schedules.

Retrieving: Retrieving is the process of preparing the located records for rendering and viewing.

1. Introduction

Information Communication Technology remain a critical driver in the management of Government Information. Guidelines for management of Government electronic records are necessary for improving the efficiency of service delivery in Public Bodies. The use of Electronic Records has broadened the scope of accessibility of public information and services by citizens and facilitated the ease of doing business in Zambia.

Certainly, online transactions generate electronic records that are provided and managed by ICT professionals. For effective management of reliable records in digital format, among the critical success factors is the implementation of proper business information systems.

This document outlines the Electronic Records and Data Management Guidelines for Public Bodies. These guidelines encompass various essential aspects of electronic records and data management, providing a framework for efficient, secure, and compliant practices. This guideline covers critical areas such as accessibility, leadership and governance, records classification, access controls, training, compliance, and continuous improvement. The implementation of this guideline aims to enhance its ability to manage electronic records effectively, streamline information retrieval, ensure data security, and promote accountability and transparency in Electronic Records Management.

1.1 Purpose of the Document

The purpose of this document is to establish comprehensive guidelines for the effective management of Electronic Records and Data within Public Bodies. It aims to ensure the secure, accessible, and compliant handling of electronic records and data throughout their lifecycle. By implementing these guidelines, the e-Government Division seeks to streamline its records management processes, enhance data integrity, promote efficient information retrieval, and adhere to legal and regulatory requirements.

1.2 Scope and Objectives

The scope of these guidelines encompasses all electronic records and data generated, received, or managed by Public Bodies, regardless of format or source. This includes but is not limited to emails, documents, databases, audiovisual files, and web content.

The objective of this Guideline is to provide a framework that ensures that;

a. Public Bodies establish a clear and consistent framework for managing electronic records and data from creation to disposal;
b. Public Bodies define roles, responsibilities, and accountability for various stakeholders involved in the management of electronic records and data.
c. Public Bodies ensure compliance with relevant laws, regulations, and industry standards concerning records management, data privacy, and information security.
d. Public Bodies optimise the accessibility, reliability, and accuracy of electronic records and data for authorised users.
e. Public Bodies minimise data redundancy and ensure efficient use of storage resources.
f. Public Bodies implement robust security measures to safeguard electronic records and data from unauthorised access, modification, or disclosure.
g. Public Bodies facilitate seamless integration of electronic records and data management practices with existing organisational processes and systems and
h. Public Bodies foster a culture of awareness and compliance among employees regarding electronic records and data management best practices.

1.3 Key Stakeholders and Responsibilities

1.3.1 Public Service Records and Data Management Committee

a. The Public Bodies shall establish a Data Management Committee that will oversee the implementation of electronic records and data management policies and procedures.
b. The Public Bodies shall review and approve records retention schedules and disposal guidelines.
c. The Public Bodies shall Provide guidance on compliance and regulatory matters related to electronic records and data management.

1.3.2 Heads of ICT in the Public Bodies or equivalent

a. Shall ensure the allocation of necessary resources for the implementation of institutional electronic records and data management guidelines.
b. Shall collaborate with the Data Management Committee to align records management strategies with the organisation's overall ICT strategy.

1.3.3 Data Stewards

a. Shall identify and assign appropriate metadata to electronic records and data for effective categorisation and retrieval.
b. Shall ensure the accuracy and quality of data under their purview and implement data cleansing processes as necessary.

1.3.4 ICT Department in the Public Bodies

a. Shall provide technical support for the implementation and maintenance of electronic records and data management systems.
b. Shall collaborate with the Public Service Records and Data Management Committee to implement security controls and data backup procedures.

1.3.5 Public Service Employees

a. Shall comply with the established electronic records and data management guidelines and procedures.
b. Shall take responsibility for the proper creation, classification, and storage of electronic records and data.

1.3.6 Legal and Standards and Compliance Officers in Public Bodies

a. Shall advise on legal and regulatory requirements related to electronic records and data management.
b. Shall assist in the development of policies and procedures to ensure compliance with relevant laws and regulations.

2. Data Accessibility

2.1. Data Privacy confidentiality and security

a. The Public Bodies shall implement robust data privacy measures to safeguard sensitive information and personally identifiable data of citizens.
b. The Public Bodies shall develop a data classification framework to categorise data based on its sensitivity and define appropriate access controls.
c. The Public Bodies shall conduct regular security audits and risk assessments to identify vulnerabilities and address potential threats to electronic records and data.

2.2. Data Retention and Disposal Guidelines

a. The Public Bodies shall develop standardised records retention schedules for different types of electronic records in accordance with legal requirements and administrative needs.

b. The Public Bodies shall establish protocols for secure and timely disposal of obsolete or redundant electronic records in compliance with retention schedules and data protection laws.

c. The Public Bodies shall adopt and use records retention and disposal schedules in compliance with the laws especially: -

   i. The National Archives Act, Cap 175 of 1995 and related regulations;
   ii. The Public Finance Act, no 15 of 2004;
   iii. The Public Service Records Management Policy of 2012;
   iv. The Registry Service Manual; and
   v. Government administrative instructions on digitization of official records 2023.

2.3. Accessibility and Usability of the Electronic Records and Data Management (ERDM) System

a. The Public Bodies shall design and implement user-friendly interfaces and search capabilities to ensure easy accessibility and retrieval of electronic records and data by authorised personnel.

b. The Public Bodies shall promote the use of open data formats and standards to enhance interoperability and usability across government systems and departments.

c. The Public Bodies shall conduct training programs and workshops to familiarise Public Service employees with the guidelines and best practices for effective utilisation of electronic records and data.

2.4. Normative References

The Guideline contains provisions which, through the references in this text, constitute provisions of this Guideline. All Guidelines are subject to revision and, since any reference to a guideline is deemed a reference to the latest edition of that guideline, parties to agreements based on this guideline are encouraged to take steps to ensure the use of the most recent editions of the guidelines. Information on currently valid national and international Standards can be obtained from the International Standards Organisation (ISO), the International Telecommunication Union (ITU), and the Zambia Bureau of Standards (ZABS). It is essential to consult with relevant stakeholders, including legal experts, data protection authorities, IT professionals, and government officials from various ministries, to ensure a comprehensive and robust policy framework that adheres to the unique needs and requirements of the Public Service landscape.

2.5. Public Electronic Records Accessibility for Persons with Disabilities

In alignment with the pertaining regulatory framework, Public documents must be accessible to persons with disabilities. To comply with this existing requirement, departments need to address how public information will be made accessible to persons with disabilities.

1. Electronic records must be formatted in accordance with manufacturers' directions related to accessibility in a format that is verifiably accessible to persons to disabilities. The following is a non-exhaustive list of formats that are accessible to persons with disabilities when applied correctly: a. .doc

a) .pdf
b) .html
c) .xml
d) .txt
e) . asci

2. In those special cases where preservation of the appearance of the original document is of legal or historic significance and it is not possible to both make the document accessible and preserve its original appearance, accessibility shall be accomplished by creation and retention of a second accessible document.

STANDARDS FOR ELECTRONIC RECORDS AND DATA MANAGEMENT GUIDELINE		
STANDARD CODE	STANDARD TITLE	YEAR
ISO 15489-1:2016	ISO 15489-1:2016 defines the concepts and principles from which approaches to the creation, capture and management of records are developed.	Uncatalogued
ISO 14641:2018	Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications.	Uncatalogued
ISO 16175-1:2020	Information and documentation — Processes and functional requirements for software for managing records — Part 1: Functional requirements and associated guidance for any applications that manage digital records.	Uncatalogued
ISO/TR 13028:2010	Establishes guidelines for creating and maintaining records in digital format only, where the original paper, or other non-digital source record, has been copied by digitising; establishes best practice guidelines for digitisation to ensure the trustworthiness and reliability of records and enable	Uncatalogued

	consideration of disposal of the non-digital source records; establishes best practice guidelines for the trustworthiness of the digitised records which may impact on the legal admissibility and evidential weight of such records; establishes best practice guidelines for the accessibility of digitised records for as long as they are required; specifies strategies to assist in creating digitised records fit for long-term retention; and establishes best practice guidelines for the management of non-digital source records following digitisation.	
ISO 13008:2022	This document specifies the planning issues, requirements and procedures for the conversion and/or migration of digital records in order to preserve the authenticity, reliability, integrity and usability of such records as evidence of business functions, processes, activities and transactions.	Uncatalogued
ISO/TR 22428-1:2020	This document presents a model for cloud records management and outlines the risks and issues that are considered by records managers before adopting cloud services for records management. The model for cloud records management includes a stakeholder model, processes, metadata, architecture, and use cases. Risks and issues are classified into those originating from cloud services internally and those originating from cloud services externally. Internal risks are associated with cloud services, systems and stakeholders. External risks and issues can occur in the social and legal context in which cloud services operate.	Uncatalogued
ISO 9735 (All parts)	Electronic data interchange for administration, commerce and transport (EDIFACT) – Application-level syntax rules	Gazetted
ISO 27010	Information security management for inter-sector and inter-organisational communications.	Gazetted
ISO 27011	Information security management guidelines for telecommunications organisations based on ISO 27002	Gazetted
ISO 14721:2012	ISO 14721:2012 defines the reference model for an open archival information system (OAIS). An OAIS is an archive, consisting of an organisation, which may be part of a larger organisation, of people and systems that has accepted the responsibility to	Gazetted

	preserve information and make it available for a designated community. It meets a set of such responsibilities as defined in this International Standard, and this allows an OAIS archive to be distinguished from other uses of the term "archive".	
ISO 18308:2011	ISO 18308:2011 defines the set of requirements for the architecture of a system that processes, manages and communicates electronic health record (EHR) information: an EHR architecture. The requirements are formulated to ensure that these EHRs are faithful to the needs of healthcare delivery, are clinically valid and reliable, are ethically sound, meet prevailing legal requirements, support good clinical practice and facilitate data analysis for a multitude of purposes.	Catalogued
ISO 13606-4	This document describes a methodology for specifying the privileges necessary to access EHR data. This methodology forms part of the overall EHR communications architecture defined in ISO 13606-1.	Gazetted
ITU-T F.743.21	Recommendation ITU-T F.743.21 defines a data asset management framework with its corresponding objects, activities and supports. Objects of data asset management are data assets, which include master data, metadata, and other data assets. Activities include data standards management, data model management, data quality management, data security management, data valuation management, and data sharing management. To ensure the proper level of management, the corresponding people in charge, rules and regulations, and technology tools are needed.	Uncatalogued
ITU-T Y.3055	Recommendation ITU-T Y.3055 provides a framework for trust-based personal data management. It introduces the necessity of trust-based personal data management based on the analysis of personal data management.	Uncatalogued
ISO/IEC 15948:2004	Information technology – Computer graphics and image processing – Portable Network Graphics (PNG): Functional specification Specifies a data stream and an associated file format, Portable Network Graphics	Catalogued

	(PNG, pronounced "ping"), for a lossless, portable, compressed individual computer graphics image transmitted across the Internet.	
ISO/IEC 19785-1: 2020	Information technology -- Common Biometric Exchange Formats Framework Part 1: Data element specification This document defines: — Structures and data elements for biometric information records (BIRs); — The concept of a domain of use to establish the applicability of a standard or specification that conforms with CBEFF requirements; — The concept of a CBEFF patron format, which is a published BIR format specification that complies with CBEFF requirements, specified by a CBEFF patron; — The abstract values and associated semantics of a set of CBEFF data elements to be used in the definition of CBEFF patron formats;	Catalogued
ISO/IEC 19784-1: 2018	Information technology – Biometric application programming interface Part 1: Bio API specification Defines the Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that support the provision of that biometric system using components from multiple vendors. It provides interworking between such components through adherence to this and to other International Standards.	Catalogued
ISO/IEC 19785-2: 2006	Information technology — Common Biometric Exchange Formats Framework Part 2: Procedures of the operation of the Biometric Registration Authority Specifies the procedures to be followed by the Biometric Registration Authority in preparing, maintaining, and publishing registers of identifiers for biometric organisations, CBEFF patron formats, BDB formats, security block formats, and biometric products	Catalogued

ISO/IEC 19785-4	Information technology – Common Biometric Exchange Formats Framework – Part 4: Security block format specifications This part specifies security block formats (see ISO/IEC 19785-1) registered in accordance with ISO/IEC 19785-2 as formats defined by the CBEFF biometric organisation ISO/IEC JTC 1/SC 37, and specifies their registered security block format identifiers. NOTE: The security block format identifier is recorded in the standard biometric header (SBH) of a patron format (or defined by that patron format as the only available security block format).	Catalogued
ISO/IEC 19792: 2009	Information technology -- Security techniques -- Security evaluation of biometrics This Standard specifies the subjects to be addressed during a security evaluation of a biometric system. It covers the biometric-specific aspects and principles to be considered during the security evaluation of a biometric system. It does not address the non-biometric aspects which might form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels).	Catalogued
ISO/IEC 19794-1: 2011	Information technology — Biometric data interchange formats — Part 1: Framework This part specifies: General aspects for the usage of biometric data records, The processing levels and types of biometric data structures, A naming convention for biometric data structures, and A coding scheme for format types.	Catalogued
ISO/IEC 19794-2: 2011	Information technology -- Biometric data interchange formats -- Part 2: Finger minutiae data Specifies a concept and data formats for representation of fingerprints using the fundamental notion of minutiae. It is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. It contains definitions of relevant terms, a description of how minutiae are	Catalogued

	to be determined, data formats for containing the data for both general use and for use with cards, and conformance information. Guidelines and values for matching and decision parameters are provided.	
ISO/IEC 19794-4: 2011	Information technology -- Biometric data interchange formats -- Part 4: Finger image data This part specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas. This can be used for the exchange and comparison of finger image data. It defines the content, format, and units of measurement for the exchange of finger image data that may be used for enrolment, verification, or identification of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, compressed or uncompressed images and vendor-specific information.	Catalogued
ISO/IEC 19794-5: 2011	Information technology -- Biometric data interchange formats -- Part 5: Face image data ISO/IEC 19794-5:2011 Specifies a record format for storing, recording, and transmitting. information from one or more facial images or a short video stream of facial images, Specifies scene constraints of the facial images, Specifies photographic properties of the facial images, Specifies digital image attributes of the facial images, and Provides best practices for the photography of faces.	Catalogued
ISO/IEC 19794-6: 2011	Information technology -- Biometric data interchange formats -- Part 6: Iris image data This part specifies iris image interchange formats for biometric enrolment, verification and identification systems. The image information might be stored as	Catalogued

	An array of intensity values optionally compressed with ISO/IEC 15948 or ISO/IEC 15444, or An array of intensity values optionally compressed with ISO/IEC 15948 or ISO/IEC 15444 that might be cropped around the iris, with the iris at the centre, and which might incorporate region-of-interest masking of non-iris regions.	
ISO/IEC 19794-8: 2011	Information technology -- Biometric data interchange formats Part 8: Finger pattern skeletal data This part specifies the interchange format for the exchange of pattern-based skeletal fingerprint recognition data. The data format is generic in that it can be applied and used in a wide range of application areas where automated fingerprint recognition is involved. This part also specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to the interchange format for the exchange of pattern-based skeletal fingerprint recognition data	Catalogued
ISO/HL7 10781: 2015	Health Informatics — HL7 Electronic Health Records-System Functional Model, Release 2 (EHR FM) Provides a reference list of functions that may be present in an Electronic Health Record System (EHR-S). The function list is described from a user perspective with the intent to enable consistent expression of system functionality.	Catalogued
SS ATSM E1769	Standard guide for properties of electronic health records and record systems	Catalogued
SS ISO 13606-4:2019	Health informatics- Electronic health record communication- Part 4: Security Describes a methodology for specifying the privileges necessary to access EHR data.	Catalogued
SS ISO 18308:2011	Health informatics- Requirements for an electronic health record architecture. Defines the set of requirements for the architecture of a system that processes, manages and communicates electronic health record (EHR) information: an EHR architecture.	Catalogued

3. Governance Structure

3.1 Establishment of a Public Service Electronic Records and Data Management Committee

a. A Public Service Electronic Records and Data Management Committee comprising representatives from relevant government departments as the EGD National Coordinator may determine including ICT, Legal and Compliance.

b. Shall designate a Public Service Electronic Records and Data Management Committee Chairperson responsible for overseeing the committee's activities and ensuring its effectiveness.

3.2 Roles and Responsibilities of Public Service Electronic Records and Data Management Committee Members

a. The Chairperson shall provide leadership and guidance to the committee, set meeting agendas, and facilitate decision-making processes.

b. The Electronic Records and Data Management Experts shall offer subject matter expertise in records and data management practices, contribute to policy development, and assist in the implementation of the guidelines.

c. The ICT Representatives shall advise on the technical aspects of electronic records and data management systems, ensure their integration with existing IT infrastructure, and address any technical challenges.

d. The Legal and Standards and Compliance Advisors shall provide legal insights and ensure that the guidelines align with relevant laws, regulations, and data protection requirements.

e. The Departmental Representatives shall act as liaisons between the committee and their respective departments, disseminate information, and gather feedback.

3.3 Decision-Making Processes

a. The Public Bodies shall adopt a consensus-based decision-making approach to ensure all committee members' perspectives are considered.

b. The Public Bodies shall schedule regular meetings to discuss policy development, implementation progress, and any emerging issues related to electronic records and data management.

c. The Public Bodies shall document meeting minutes and action items to keep track of decisions made, tasks assigned, and deadlines.

3.4 Reporting and Accountability Mechanisms

a. The Public Bodies shall establish a reporting framework to keep government leadership and relevant stakeholders informed about the Electronic records and data management activities and progress.
b. The Public Bodies shall prepare regular progress reports highlighting milestones achieved, challenges faced, and recommendations for improvement.
c. The Public Bodies shall ensure transparency in decision-making processes and be accountable for the successful implementation of the Electronic Records and Data Management Guidelines.
d. The Public Bodies shall collaborate with internal audit and standards and compliance departments to conduct periodic assessments of adherence to the guidelines and identify areas for enhancement.

4. Records Classification and Metadata Standards

4.1 Definition of Record Types

a. The Public Bodies shall define and categorise various types of electronic records based on their content, purpose, and business value.
b. The Public Bodies shall Identify common record types across government departments and tailor specific classifications as needed for each department's unique records.

4.2 Metadata Elements for Records Identification

a. The Public Bodies shall establish a standardised set of metadata elements to be captured for each electronic record. These may include:
   i. Title/Description: A concise and informative title or description of the record's content.
   ii. Author/Creator: The individual or entity responsible for creating the record.
   iii. Date of Creation: The date when the record was originally created.
   iv. Date of Last Modification: The date when the record was last modified or updated.
   v. Record Identifier: A unique identifier assigned to the record for easy tracking and retrieval.
   vi. Record Type: The category or classification of the record.

vii. Access Restrictions: Indicate any access controls or restrictions applicable to the record.

4.3 File Naming Conventions

a. The Public Bodies shall establish a consistent and logical file naming convention to ensure uniformity and ease of identification for electronic records.
b. The Public Bodies shall Include relevant metadata elements in the file name to enable quick recognition and organisation (e.g., Record_Type_Title_Date).

4.4 Indexing and Search Capabilities

a. The Public Bodies shall implement a comprehensive indexing system that allows for efficient and accurate searching of electronic records based on their metadata.
b. The Public Bodies shall integrate indexing capabilities with the electronic records management system to enable rapid retrieval of relevant records.
c. The Public Bodies shall train employees in effective search techniques to enhance their ability to locate specific records when needed.

4.5 ERDM System

These are systems acquired for the management of Electronic Records throughout their life cycle. Below are guidelines to be considered when acquiring an ERDMS.

a. Should be able to capture records in bulk.
b. It should be able to import and export records.
c. electronic records in their existing format, without degradation of content or structure, retaining any contextual relationships between the components of any individual record;
d. electronic records and all associated records management metadata, retaining the correct contextual relationships between individual records and their metadata attributes;
e. The structure of aggregations to which the records are assigned, and all associated metadata, retaining the correct relationship between records and aggregations and

f. Be able to import any directly associated event history metadata with the record and/or aggregation, retaining this securely within the imported structure.
g. Be able to track, monitor and record information about location and movement of Electronic Records.

4.6 Electronic document formats ERDM System

a. Support the capture of records created in native file formats from commonly used software applications such as:
   i. guideline office applications (word processing, spread-sheeting, presentation, simple databases);
   ii. email client applications; imaging applications;
   iii. Architectural Computer-Aided Design (CAD) Drawings;
   iv. Web authoring tools.
b. Be able to extend the range of file formats supported as new file formats are introduced for business purposes or for archival retention

NOTE: The ERDMS must be able to support the creation of an infinite number of document types.

5. Records Creation and Capture

5.1 Guidelines for Creating Electronic Records

a. The Public Bodies shall provide clear guidelines and training to government employees on the proper and consistent creation of electronic records.
b. The Public Bodies shall emphasise the importance of accurate and complete metadata entry during the record creation process.
c. The Public Bodies shall encourage the use of standardised templates and forms for specific types of records to ensure uniformity and ease of organisation.

5.2 Data Entry Standards

a. In data entry Public Bodies shall ensure data integrity and data consistency across electronic records.
b. The Public Bodies shall define data validation rules to minimise errors during data entry and ensure data accuracy.
c. The Public Bodies shall implement measures to prevent duplicate records and maintain a clean database of electronic records.

5.3 Capturing Records from Various Sources

a. The Public Bodies shall integrate electronic records capture mechanisms with existing communication tools like email clients to automatically capture important correspondence as records.
b. The Public Bodies shall utilise authorised document management systems that can capture and organise electronic documents as official records.
c. The Public Bodies shall develop procedures for capturing data from databases and other electronic sources, ensuring that the data remains reliable and up to date.

5.4 Automation and Integration with Business Processes

a. The Public Bodies shall continuously identify opportunities for automation in the records creation and capture process to reduce manual efforts and potential errors.
b. The Public Bodies shall integrate the electronic records management system with relevant business processes to enable seamless capture and classification of records.
c. The Public Bodies shall ensure that the integration of electronic records management aligns with existing workflows and enhances overall efficiency.

6. Records Storage and Preservation

6.1 Selection of Appropriate Storage Solutions

a. The Public Bodies shall assess the storage needs of electronic records based on their volume, sensitivity, and access requirements.
b. The Public Bodies shall implement a tiered storage approach, categorizing records based on their frequency of use and archival value.
c. The Public Bodies shall choose reliable and secure storage solutions, including on-premises servers, cloud-based storage, and off-site backup facilities.
d. All records generated within a Public Body shall be stored on the provided relevant official public infrastructure.

6.2 Backup, Disaster Recovery, and Business Continuity Procedures

a. The Public Bodies shall develop and implement regular backup procedures to safeguard electronic records from data loss due to hardware failures, cyber-attacks, or natural disasters.

b. The Public Bodies shall establish a comprehensive Disaster Recovery and Business Continuity plan outlining steps to recover and restore electronic records in case of system outages or catastrophic events.
c. The Public Bodies shall conduct periodic drills and simulations to test the effectiveness of backup and recovery procedures.

6.3 Long-term Preservation Strategies

a. The Public Bodies shall identify electronic records of enduring historical, legal, or cultural value that require long-term preservation.
b. The Public Bodies shall implement digital preservation strategies, such as migration to new formats or technologies, to ensure the accessibility and usability of records over time.
c. The Public Bodies shall collaborate with archival institutions or specialised preservation experts for the management of records with significant historical importance.

6.4 Migration and Format Conversion Guidelines

a. The Public Bodies shall establish guidelines for the migration of electronic records to newer storage technologies or formats to prevent data loss and obsolescence.
b. The Public Bodies shall ensure data integrity and accuracy during migration processes, including verification and validation procedures.
c. The Public Bodies shall develop procedures for format conversion of legacy records, preserving their content and context in the new format.

7. Data Management and Quality Assurance

7.1 Data Governance and Data Stewardship

a. The Public Bodies shall establish a clear data governance framework with defined roles and responsibilities for data management.
b. The Public Bodies shall assign data stewards who will be responsible for overseeing data quality, integrity, and compliance within their respective departments.
c. The Public Bodies shall Develop data governance policies that outline data ownership, accountability, and decision-making processes.

7.2 Data Quality Standards and Validation Processes

a. The Public Bodies shall define data quality standards, including accuracy, completeness, consistency, and timeliness, for electronic records and data.

b. The Public Bodies shall implement data validation processes to ensure that electronic records meet the established data quality standards.
c. The Public Bodies shall conduct regular data quality assessments and audits to identify and address data issues proactively.

8. Compliance and Auditing

8.1 Regular Compliance Audits

a. The Public Bodies shall conduct regular compliance audits of the electronic records and data management system to assess adherence to the established guidelines, policies, and procedures.
b. The Public Bodies shall appoint a dedicated team or engage external auditors with expertise in records management and data governance for conducting audits.
c. The Public Bodies shall document audit findings, including areas of non-compliance and potential risks, and create action plans for addressing identified issues.

8.2 Remediation and Corrective Actions

a. The Public Bodies shall implement remediation measures and corrective actions to address issues identified during compliance audits promptly.
b. The Public Bodies shall assign responsibilities for remediation to relevant stakeholders and set clear timelines for resolution.
c. The Public Bodies shall monitor and track progress on corrective actions to ensure timely completion and effectiveness.

8.3 Reporting to Regulatory Authorities

a. The Public Bodies shall prepare and submit regular compliance reports to relevant regulatory authorities e.g. Auditor General and Data Commissioner's Office, as required by applicable laws and regulations.
b. The Public Bodies shall include details on the implementation status of the electronic records and data management guidelines, audit findings, and actions taken for remediation.
c. The Public Bodies shall establish communication channels with regulatory authorities to address any inquiries or requests related to records management compliance.

8.4 Data Cleansing and De-duplication

a. Public Bodies shall develop data cleansing procedures to identify and correct errors, inconsistencies, and redundancies in electronic records and data.
b. The Public Bodies shall implement de-duplication processes to eliminate duplicate records and optimise data storage resources.
c. The Public Bodies shall establish protocols for regular data maintenance and cleansing to maintain data accuracy and reliability.

8.5 User Interfaces, Mobile Working and Remote Access

a. The user interface of the Solution shall be well-designed, easy to use, and intuitive user interface.
b. Remote Access to Electronic Records management systems by data stewards shall be via a secured connection such as Virtual Private Network (VPN).
c. All public-facing user interfaces shall be secured, e.g., Secure Socket Layer (SSL) certificate for web servers.

9. Access and Security Controls

9.1 User Authentication and Authorisation

a. The Public Bodies shall implement strong user authentication methods, such as multi-factor authentication, to verify the identity of users accessing electronic records and data.
b. The Public Bodies shall establish access control policies that define user privileges based on job roles and responsibilities.
c. The Public Bodies shall regularly review and update user access rights to ensure that access permissions align with current roles and requirements.
d. The Electronic Records Management System must be developed with the capabilities to manage Classified Records as prescribed in the Government Office Instructions Manual.
e. Authenticity of Electronic Records shall be verified using prescribed Electronic Signature methods.

9.2 Role-based Access Controls

a. The Public Bodies shall adopt a role-based access control (RBAC) model to assign access rights and permissions based on predefined roles and responsibilities.

b. The Public Bodies shall define different user roles with specific access levels, ensuring that individuals can only access the electronic records necessary for their job functions.
c. The Public Bodies shall conduct periodic access reviews to verify that users' access rights are appropriate and in line with their roles.

9.3 Encryption and Data Protection Measures

a. The Public Bodies shall encrypt sensitive electronic records and data both in transit and at rest to safeguard them from unauthorised access or interception.
b. The Public Bodies shall implement data loss prevention (DLP) measures to prevent sensitive information from being inadvertently shared or leaked.
c. The Public Bodies shall establish data protection policies that comply with relevant data protection laws and regulations.

9.4 Monitoring and Logging

a. The Public Bodies shall deploy a comprehensive monitoring and logging system to track user activities and access attempts to electronic records and data.
b. The Public Bodies shall regularly review and analyse logs to detect any suspicious or unauthorised access attempts.
c. The Public Bodies shall establish incident response protocols to address and mitigate security breaches promptly.

10. Training and Awareness

10.1 Training Programs for Records and Data Management

a. The Public Bodies shall develop comprehensive training programs on electronic records and data management for Public Service employees at all levels of the Public Bodies.
b. The Public Bodies shall tailor training sessions to different user groups, addressing their specific roles and responsibilities in managing electronic records and data.
c. The Public Bodies shall cover topics such as record creation, metadata entry, data quality assurance, security protocols, and compliance with data management policies.

10.2 Awareness Campaigns for Public Service Employees

a. The Public Bodies shall launch awareness campaigns to promote the importance of proper electronic records and data management among all Public Service employees.
b. The Public Bodies shall utilise various communication channels, such as emails, newsletters, intranet, and posters, to disseminate key messages about the guidelines and best practices.
c. The Public Bodies shall highlight the benefits of effective records management, including improved efficiency, data accuracy, and compliance with legal requirements.

10.3 Ongoing Support and Learning Resources

a. The Public Bodies shall provide ongoing support for employees to address their questions, challenges, and feedback related to electronic records and data management.
b. The Public Bodies shall establish a dedicated help desk or support team to assist employees in navigating the electronic records management system and addressing technical issues.
c. The Public Bodies shall develop and maintain a repository of learning resources, including user guides, video tutorials, and FAQs, to facilitate continuous learning and skills development.

11. Records Retention and Disposal

11.1 Retention Schedules and Legal Requirements

a. The Public Bodies shall develop comprehensive records retention schedules that outline the appropriate retention periods for different types of electronic records based on legal, regulatory, and administrative requirements.
b. The Public Bodies shall collaborate with legal experts to ensure that the retention schedules align with relevant laws and regulations governing records management in Public Bodies.
c. The Public Bodies shall regularly review and update the retention schedules to reflect any changes in laws or institutional needs.

11.2 Disposal Procedures for Obsolete Records

a. The Public Bodies shall establish clear and standardised procedures for the disposal of obsolete electronic records at the end of their designated retention periods.
b. The Public Bodies shall ensure that disposal processes comply with legal and regulatory requirements, including data protection and privacy laws.
c. The Public Bodies shall conduct regular audits to identify records that have reached their retention end dates and require proper disposal.

12. Performance Measurement and Continuous Improvement

12.1 Key Performance Indicators (KPIs) for Records and Data Management

a. The Public Bodies shall define key performance indicators (KPIs) that align with the objectives of the Electronic Records and Data Management Guidelines.

KPI examples may include:

i. Data accuracy and integrity rates.
ii. Compliance with retention schedules and disposal procedures.
iii. Timeliness of records retrieval and response to information requests.
iv. User satisfaction with the electronic records management system.
v. Number of security incidents and response time to resolve them.

12.2 Monitoring and Evaluation Processes

b. The Public Bodies shall establish a systematic monitoring and evaluation framework to track progress toward meeting the defined KPIs.
c. The Public Bodies shall conduct regular assessments and audits to evaluate the effectiveness of the electronic records and data management practices.
d. The Public Bodies shall analyse data and performance trends to identify areas of improvement and best practices.

12.3 Feedback Mechanisms for Process Improvement

a. The Public Bodies shall create feedback mechanisms, such as surveys or suggestion boxes, to gather input from employees and stakeholders on the effectiveness of the guidelines.

b. The Public Bodies shall encourage open communication and collaboration among users, ICT, and records management teams to share insights and challenges.
c. The Public Bodies shall utilise feedback to identify opportunities for process improvement and inform updates to the Electronic Records and Data Management Guidelines.

13. Integration with Existing Systems and Processes

13.1 Seamless Integration with Business Applications

a. The Public Bodies shall identify critical business applications used across government departments and assess their compatibility with the electronic records management system.
b. The Public Bodies shall collaborate with ICT and business process owners to seamlessly integrate the records management system into existing applications, minimising disruption to daily workflows.
c. The Public Bodies shall ensure that the electronic records management system supports common file formats and is capable of capturing records from various applications.

14. Email Management in Public Bodies

14.1 Components of a complete record

a. A complete email record must incorporate the address, identify the intended recipient(s), salutation and the message content. The message should consist of: identification of the sender, meaningful subject line, closing remarks and signature block.

14.2 Consistent formatting

a. Establish a consistent and clear format for including the document reference number in the subject line of the email. This format should be adhered to across all Public Bodies and Public Service employees.

14.3 Handling Attachments and Draft Emails

a. Email attachments may be integrated directly into the Public Bodies or the user's filing system, multiple attachments or attachments in multiple formats may be associated with an individual message, or the body of the message itself may contain information associated with the attachments.

i. If the electronic message is a record and contains attachments, the attachments must be retained as part of the record. Retention should be defined by the longer of the retention requirements for the message or the retention requirements for the attachment.
ii. If the Public Bodies transmits attachments via email, when possible, consider placing the documents on a shared drive or making them available across a storage area network.
iii. Draft emails should not be retained as official record copies because they do not represent the final, authorized position of the institution. Draft emails should be purged immediately after the final version has been approved.

14. 4 Electronic Transmission of Confidential and Sensitive Information

a. Public Service employees should always obtain clearance from the Supervisor to use email to communicate confidential or sensitive records.

14. 5 Etiquette and Communication Standards

a. When creating records using email, Public Service employees should follow standards for formal business communications, i.e., use standard business letter layout, business language, and proper grammar and punctuation.

14.6 Backup and Archiving

a. Public Bodies shall establish centralised email servers for backups and archives to store and organise electronic communications and attachments.
b. Electronic Records shall adhere to the National Archives Act Chapter 175 of the Laws of Zambia.
c. Public Bodies shall use prescribed media for archiving electronic records.

14.6 Security, Confidentiality and Encryption

a. Public Bodies should implement robust security measure for email communication that ensures the confidentiality, integrity, and authenticity of electronic records. Encryption, access controls, and regular security audits should be essential components of a secure email system.

15. Appendix A: Electronic Records Management Technical Committee

This committee shall support and assist the MPSA information/record custodians and information service providers in adherence to E-Records Management Guideline, and ensure adherence to established legal, statutory and regulatory requirements: -

a. Advice the Controlling Officer on information and records management matters.
b. Ensure awareness, training, adoption, and implementation of the ERDM Guideline
c. Ensure the development and implementation of information and records management policy and procedures.
d. This committee shall oversee the management of records in an Public Bodies.
e. The committee shall ensure that annual surveys and audits determine the state of records management in the Public Bodies.
f. Also, the committee will be responsible for constituting any Task Force and or ad hoc committee herein mentioned.
g. The Technical Committee shall have representation from ICT, Records, Finance, Administration, and Procurement departments.
h. Committee meetings will be convened at least once every quarter.
i. The Technical Committee shall interface with other relevant committees.
j. Shall have quarterly meetings and not less than 4 in a financial year.

16. Appendix B: Conformity Assessment Checklist

Sub-topic	Details	Rating		
		YES	NO	%
6.1 General	6.1.2 Public Bodies maintain an Electronic Records Management Policy.			
	6.1.3 Public Bodies provides training and adequate support to ensure users understand and implement ERDM system procedures.			
	6.1.4 Public Bodies maintains clear procedures and processes for the receipt, creation, processing, and filing and disposition of e records. Also, any other documentation relevant to management of e-records has been maintained.			
	6.1.5 The Public Bodies clearly defines the roles and			
	responsibilities of the human resource managing E-records and ERDMS.			
	6.1.6 Records are classified using the GRS classification scheme – secret, top secret, restricted, confidential			
6.2 Capturing of Electronic Records	6.2.1 Public Bodies designates a receiving device(s) for electronic records. This supports export, import or migration of the records.			
6.3 Classification and Indexing	6.3.1 Public Bodies has established, implemented and maintained a business classification scheme			
	6.3.2 Records classification has been applied to individual records, or at any level of aggregation. E-records that are reclassified during their retention period, the superseded classification metadata have been retained.			
	6.3.3 Indexing metadata has been linked with records at the point of capture, and/ or added as required throughout their existence			

6.4 Access Control and Storage	6.4.1 Public Bodies has: a. Defined the rights of access, permissions and restrictions as applicable b. defined roles and responsibilities of individuals involved in e records creation, maintenance, and disposition c. Maintained physical and environmental security controls. d. Maintained logical access control mechanisms			
	6.4.2 Public Bodies has deployed an ERDM system that has controlled storage or filing systems that maintain the integrity and accessibility of			
	E-records; and that allow all records, volumes and aggregation records to be retrievable through searching and navigation.			
	6.4.3 PUBLIC BODIES has maintained problem-resolution procedures including incident reporting and response procedures			
	6.4.5 Public Bodies has maintained a contingency plan that has include but not limited to data backup, disaster recovery and business continuity			
6.5 Migration and Conversion	6.5.1 Public Bodies has a planned, documentation and communication process of migration and conversion between business and/or records systems, including the decommissioning of the system(s), or from paper to digital formats (digitisation), to internal and external stakeholders.			
	6.5.2 The disposition of source records following a migration or conversion process is authorised.			

	6.5.3 During migration or conversion, all record content and its associated metadata in the originating system or format is retained until the process is finished and the integrity and reliability of the destination system or format have been controlled and secured.			
	6.5.4 Migration or conversion processes are audited, authorised or certified by an ad-hoc committee (that may include internal and external stakeholders).			
6.6 Retention and Disposal	6.6.1 Public Bodies has adopted and used records retention and disposal schedules in compliance with the laws especially; (a) Public Records and Archives Administration Act - 1997 (Act 535) (b) III. The Public Finance Act, no 15 of 2004; (c) E-waste Standards and Guidelines (d) Data Protection Act 2012			
	6.6.2 Public Bodies ensures that electronic records management systems use guideline formats to help reduce the rate of technological obsolescence and the need for migration			
	6.6.3 Public Bodies has put in place measures to ensure the continued usability of E-records during their retention period. These measures may include: (a) applying and maintaining appropriate and persistent metadata about a record's technical dependencies; (b) Additional copies of records or converting them into alternative formats; (c) Migrating records; (d) Retain documented information on routine monitoring of storage conditions			

	6.6.4 The following disposal action may be applicable; (a) Destruction of records and metadata; (b) Transfer of control of records and metadata to an organisation that has assumed responsibility for the business activity through restructure, sale, privatisation or other business change; (c) Transfer of control of records and metadata to an institutional or external archive for permanent retention.			
6.7 Electronic Records and Data Management Systems	6.7.1 Electronic Records Management Systems effectively supports creation, maintenance and disposition of Electronic Records.			
	6.7.2 Public Bodies has acquired ERDM products and services systems in accordance with: (a) Systems and ICT Assets Acquisition Guidelines. (b) Office Equipment Standards and Guideline			
	6.7.3 The functional requirements of ERDM systems.			
6.8 Business Applications	6.8.1 All business Applications are able to; 6.8.2 (a) Create, manage, maintain electronic records, and (b) Support import, export and interoperate with an e-records management system.			