GOVERNMENT ICT STANDARDS

Electronic Records Management Standard

ICTA-4.1.003:2023

The ICT Authority is a State Corporation under the State Corporations Act 446
www.icta.go.ke

REVISION OF ICT STANDARDS

In order to keep abreast of progress in industry, ICT Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Chief Executive Officer, ICT Authority, are welcome.

ICT AUTHORITY (ICTA)

Telposta Towers 12th floor. Kenyatta Avenue P.O. Box 27150-00200, Nairobi Kenya Tel.: +254 20 2089061
Web:http://www.icta.go.ke
Email:standards@ict.go.ke

DOCUMENT CONTROL

Document Name:	Electronic Records Management Standard
Prepared by:	Electronic Records Management Technical Committee
Edition:	Third Edition
Approved by:	Board of Directors
Date Approved:	3rd May 2023
Effective Date:	1st July 2023
Next Review Date:	After 3 years

CONTENTS

FOREWORD

The ICT Authority has the mandate to set and enforce ICT standards and guidelines across all aspects of information and communication technology including Systems, Infrastructure, Processes, Human Resources and Technology for the public service. The overall purpose of this mandate is to ensure coherent and unified approach to acquisition, deployment, management and operation of ICTs across the public service in order to achieve secure, efficient, flexible, integrated and cost-effective deployment and use of ICTs. To achieve this mandate, the Authority established a standards committee to identify the relevant standard domains and oversee the standards development process. The committee consulted and researched broadly among subject matter experts to ensure conformity to acceptable international and national industry best practices as well as relevance to the Kenyan public service. The committee eventually adopted the Kenya Bureau of Standards (KEBS) format and procedure for standards development. In an engagement founded on a memorandum of understanding KEBS, participated in the development of these Standards and gave invaluable advice and guidance. The Electronic Records Management Standard, which falls under the overall Government Enterprise Architecture (GEA), has therefore been prepared in accordance with KEBS standards development guidelines based on the international best practices by standards development organizations including International Organization for standardization (ISO). The ICT Authority in consultation with Kenya National Archives and documentation Service has the oversight role and responsibility for management, enforcement and review of this standard. The Ministries, Departments, Agencies and Counties will be audited annually to determine compliance. The Authority shall issue a certificate for compliance to agencies upon inspection and assessment of the level of compliance to the standard. For non-compliant agencies, a report detailing the extent of the deviation and the prevailing circumstances shall be tabled before the Standards Review Boardwho shall advise and make recommendations. The ICT Authority management, conscious of the central and core role that standards play in public service integration, fostering shared services and increasing value in ICT investments, shall prioritize the adoption of this standard by all Government agencies. The Authority therefore encourages agencies to adhere to this standard in order to obtain value from their ICT investments.

Stanley Kamanguya, OGW
Chief Executive Officer
ICT Authority

1.0 INTRODUCTION

Electronic government (e-government) has been considered as the use of ICTs for improving the efficiency of government agencies and providing government services online. This has since broadened to include use of ICT by government for conducting a wide range of interactions with citizens and businesses. These online government transactions generate electronic records that are provided and managed by archivists and records management professionals. Therefore, there is need for strong collaboration between records management and ICT professionals. Information is vital to the operation of government offices. All government agencies depend on electronically-generated data to accomplish their basic functions. While technology gives state and local government agencies the capability to respond to the growing demand for information, it also presents a number of concerns, including:

- Long-term retention
- Compatibility
- Accessibility
- Security

State and local government agencies must ensure government records, in any format, are managed in compliance with records laws and requirements.

This standard envisages sound management of electronic records by MCDAs to ensure they have the following inherent characteristics:

- **Authenticity –** the record can be proven to be what it purports to be, to have been created or sent by the person that created or sent it, and to have been created or sent at the time it is purported to have occurred.
- **Reliability –** the record can be trusted as a full and accurate representation of the transaction(s) to which they attest, and can be depended on in the course of subsequent transactions.
- **Integrity –** the record is complete and unaltered, and protected against un-authorized alteration. This characteristic is also referred to as 'inviolability'.
- **Usability –** the record can be located, retrieved, preserved and interpreted

Generally, records management; electronic or otherwise provides a basis for: Efficiency, effectiveness and continuity in service delivery; Transparent, informed and quality planning and decision-making; Verifiable demonstrating and account for organizational activities; Enhancing access to public information; and Maintaining the confidentiality and privacy of non-public personal information. This Standard is therefore developed to provide guidance on management of electronic records such that they meet the same requirements as their regular paper record counterparts. Thus, digital objects created by email, word processing, spread sheet and imaging applications (such as text documents, and still and moving images), where they are identified to be of business value, should be managed within electronic records management systems that meet the functional requirements in this standard. Records managed by an electronic records management system may be stored on a variety of different media formats, and may be managed in hybrid record aggregations that include both electronic and non-electronic elements.

2.0 SCOPE

This standard sets out general aspects, capture and receipt, classification and indexing, access control and security, digital conversion and migration, and retention and disposal of public electronic records (e-records).

3.0 APPLICABILITY

This Standard is applicable to:

- National Government (Ministries, Departments and Agencies),
- Constitutional Commissions and Independent Offices, and
- County Governments.

4.0 NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. All standards are subject to revision and, since any reference to a standard is deemed a reference to the latest edition of that standard, parties to agreements based on this standard are encouraged to take steps to ensure the use of the most recent editions of the standards indicated below. Information on currently valid national and international standards can be obtained from Kenya Bureau of Standards.

The normative references include:

- ISO 30300:2020. Information and documentation — Records management — Core concepts and vocabulary.
- KS ISO 30301:2019. Information and documentation - Management systems for records – Requirements
- ISO 30302:2022. Information and documentation — Management systems for records — Guidelines for implementation
- ISO 15489-1:2016: Information and documentation - Records management - Concepts and principles
- ISO/TR 15489-2:2001. Information and documentation — Records management —Guidelines.
- ISO 23081-1:2017. Information And Documentation - Records Management Processes - Metadata for Records – Principles
- ISO 23081-2:2021. Information and documentation. Metadata for managing records.
- KS ISO TR 18128:2014. Information and documentation — Risk assessment for records processes and systems
- KS ISO/TR 21946:2018. Information and documentation — Appraisal for managing records
- KS ISO 13008:2012. Information and documentation — Digital records conversion and migration process.

5.0 TERMS AND DEFINITIONS

For the purpose of this Standard the following terms and definitions will apply:

5.1 Access

Refers to rights, opportunity, means of finding, using or retrieving information;

5.2 Agent

An individual, workgroup or MDAC responsible for or involved in record creation, capture and/or records management processes;

5.3 Aggregation

Aggregation of electronic records is an accumulation of related electronic record entities that when combined may exist at a level above that of a singular electronic record object, for example a file or series;

5.4 Archives

These are collections of records that have been chosen for permanent or long-term preservation due to their cultural, historical, or evidential importance;

5.5 Business Classification Scheme

Refer to a governance tool that organizes work of MDACs by function and by activity, and helps with the proper management of records created;

5.6 Classification

This is systematic identification and arrangement of business activities and their records into categories according to logically structured conventions, methods and procedural rules;

5.7 Content

An element of record that provides basic data or information carried in a record; substance of the record that captures sufficient information to provide evidence of a business transaction;

5.8 Context

An element of record that provides the relationship of the record to the business and technical environment in which it arises;

5.9 Conversion

Process of changing records from one format to another;

5.10 Destruction

Refers to a disposal process whereby digital records, record plan entities and their metadata are permanently removed, erased or obliterated but with authorization and approval of the KNADS;

5.11 Disposition

This refers to range of processes associated with implementing records retention, destruction, transfer or long-term preservation which are documented in disposition authorities or other instruments;

5.12 Document

Refer to documented information which can change from time to time but in a controlled manner;

5.13 Electronic Documents

Refer to collection of data, which may be produced through original output, combination of existing data or data received from outside the organization such as via e-mail, or scanning;

5.14 Electronic Document Management System

This is an electronic system that can collect and organize documents for storage, retrieval, and tracking purpose. They have ability to preserve and provide access to the content, structure, and context of the records;

5.15 Electronic Records

Refer to 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;

5.16 Electronic Records Management System

An automated system used to manage the creation, use, maintenance and disposal of electronic records. An E-records management system should be able to maintain a record along with its associated metadata;

5.17 Export

This is process of passing metadata of a digital record or a group of records are from one system to another system; either within or beyond the organization;

5.18 Indexing

Refers to the process of describing and identifying documents or records in terms of their subject contents;

5.19 Long term Preservation

Refer to preservation period greater than ten (10) years;

5.20 Metadata

It is data describing the content, context, and structure of records and their management through continuum care;

5.21 Migration

This is process of moving records from one system to another, while maintaining their authenticity, integrity, reliability and usability;

5.22 Record

Refer to information created or received in any format and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business;

5.23 Records Management

Records management is an integrated framework of governance arrangements, architectures, policies, processes, systems, tools and techniques that enables organisations to create and maintain trustworthy evidence of business activity in the form of records;

5.24 Rendering

Rendering is the production of a human-readable representation of a record, usually to a visual display screen or in hardcopy format;

5.25 Retrieving

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

5.26 Redacting

The process of masking or deleting information in a record;

5.27 Structure

An element of record that provides the physical and logical format of records, where logical format includes elements such as font type, font size, margin, headers, labels; and logical format include how information is arranged;

6.0 ABBREVIATIONS AND ACRONYMS

ASCII	American Standard Code for Information Interchange
BCP	Business Continuity Plan
BS	Business System
EDMS	Electronic Document Management System
ERM	Electronic Records Management
ERMS	Electronic Records Management System
GEA	Government Enterprise Architecture
GoK	Government of Kenya
ICT	Information and Communication Technology
ISO	International Organization for Standardization
KEBS	Kenya Bureau of Standards
KS	Kenya Standard
KNADS	Kenya National Archives and Documentation Service
MCDAs	Ministries, Counties, State Departments, and Agencies
PDF	Portable Document Format
PDF/A	Portable Document Format Archive
PIN	Personal Identification Numbers
PKI	Public Key Infrastructure
RM	Records Management
SGML	Standard Generalized Markup Language
SSL	Secure Sockets Layer
TR	Technical Reports
VPN	Virtual Private Network

7.0 REQUIREMENTS

7.1 General Provisions

7.1.1 Ministries, Counties, Departments and Agencies (MCDAs) shall establish a Records Management Committee.

The committee will be responsible for advisory on design, implementation and support of electronic records management systems in accordance to relevant standards.

The Committee shall draw membership from the following functions;

(i) Records Management/ Archives management

(ii) ICT

(iii) All Technical functions

7.1.2 MCDAs shall develop and implement an electronic records management policy. Its development will take into consideration:

- Legal and regulatory requirements (see also, IT Governance standard);
- Processes and business operations;
- Business needs that should be addressed; and
- Past practices in managing paper records that can be digitized.

7.1.3 MCDAs shall build requisite capacity to implement, use and support ERM system

7.1.4 Shall provide adequate resources to support Electronic Records management as per work plans

7.1.5 MCDAs shall develop and implement clear procedures for the creation, receipt, processing, maintenance, filing and disposition of e-records.

7.1.6 The MCDA shall clearly define the roles and responsibilities for managing e-records and ERMS.

7.1.7 MCDAs shall establish, implement and maintain a business classification scheme that reflects their functions and business activities

7.2 Creation, Receipt and Capture of E-records

7.2.1 MCDAs shall develop and document clear procedures for the receipt, creation, capture, processing, and filing of electronic records

7.2.2 MCDAs shall designate a receiving device(s) for e-records. This should support export, import or migration of the records (A "device" could mean a specific server, e-mail address or website.)

7.2.3 There shall be mechanisms to authenticate senders and determine the integrity of each type of e-record

7.2.4 There shall be measures to authenticate the identity of the sender based on potential risk and legal requirements such as PIN, fingerprints, voice verification, signature dynamics, retinal scans or electronic signature dynamics

7.2.5 There shall maintain measures to document the date and time of receipt that is time stamp

There shall be means to confirm receipt of e- records

7.2.7 MCDAs shall protect the contents of records from alteration and deletion during and after records capturing with the exceptions of destruction in accordance with an approved records retention and disposal schedule and deletion by an authorized individual under very exceptional cases and in a tightly controlled manner.

7.3 Classification and Indexing of E-records

7.3.1 MCDAS shall develop and implement a records classification and indexing

7.3.2 The system must have the capability to organize records in a structured and hierarchical records classification scheme(s)

7.3.2 Records classification should be applied to individual records, or at any level of aggregation. E-records that are reclassified during their retention period, the superseded classification metadata should be retained.

7.3.3 Indexing metadata shall be linked with records at the point of capture, and/ or added as required throughout their existence (indexing metadata may include title, time, date, subjects, location or personal names)

7.3.4 MCDAs shall ensure that metadata is captured and persistently linked to the associated entity including an aggregation or a record, and be managed and maintained properly. It is always preferable to have metadata which are system-generated, automatically captured or inherited so as to minimize users' capturing efforts and avoid manual errors.

7.4 Control of Electronic Records

7.4.1 MCDAs shall design controls for processes and systems that will ensure authentic and reliable records:

- Are created through routine and repeatable processes;
- Are of undisputed origin; and
- Can be trusted to be genuine.

7.5 Access Control and Security of E-records

7.5.1 MCDAs shall protect captured records against unauthorised access; intentional or accidental alteration and deletion of their content, context and structure throughout their life cycle.

7.5.2 Access to aggregations and records and system functions shall be granted to users, user groups and/or user roles based on the business needs.

7.5.3 Records shall be classified as per the Government of Kenya Protective Security manual (2018) – Top secret, secret, confidential and restricted

7.5.4 MCDAs shall:

(i) Define the rights of access, permissions and restrictions as applicable

(ii) Define roles and responsibilities of individuals involved in e-records management in accordance to principle of separation of duties

(iii) Maintain physical and environmental security controls

(iv) Maintain logical access control mechanisms including authentication, authorization, and accountability

MCDAs shall deploy ERM systems that have 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.

7.5.6 MCDAs shall develop and implement problem resolution procedures including incident reporting and response procedures

7.5.7 MCDAs shall maintain contingency plan(s) that shall include but not limited to data backup, disaster recovery and business continuity

7.5.8 MCDAs shall ensure that use of electronic records is tightly integrated with the security and access control, meaning that users must not be allowed to access aggregations and records to which they do not have the access rights.

7.6 Digital Conversion and Migration

7.6.1 MCDAs shall maintain electronic records in a format which is expected to survive and be readable for the required life of the record.

7.6.2 Digital records shall be in a format that is expected to survive and remain accessible and readable using readily available software for the required life of the record.

7.6.3 MCDAs shall provide sufficient descriptive information attached to electronic records to allow access and management over time.

7.6.4 All electronic records shall be managed to facilitate conversion and migration or relocation over time

7.6.5 MCDAs shall plan, document and communicate the process of migration and conversion between business and/or records systems, including the decommissioning of the system(s), or from paper to digital formats (digitization), to internal and external stakeholders.

7.6.6 The disposition of source records following a migration or conversion process shall be duly authorized by the KNADS.

7.6.7 During migration or conversion, all record content and its associated metadata in the originating system or format shall be retained until the process is finished and the integrity and reliability of the destination system or format have been controlled and secured.

7.6.8 Migration or conversion processes shall be audited; authorized or certified by an ad-hoc committee (the committee may include internal and external stakeholders).

7.7 Retention and Disposal of E-records

7.7.1 MCDAs shall implement systems that have the capability to retain and dispose of records in a managed, systematic and auditable way according to pre-defined records retention and disposal schedules.

MCDAs shall develop and apply records retention and disposal schedules duly approved by KNADS

7.7.3 MCDAs shall ensure electronic records management systems use standard formats such as PDF, PDF(A), relational databases, ASCII, and SGML.

7.7.4 MCDAs shall ensure continued usability of e-records during their retention period. These measures may include: maintaining appropriate and persistent metadata about a record's technical dependencies; converting records into alternative formats; migrating records; retain documented information on routine monitoring of storage conditions.

7.7.5 MCDAs in liaison with KNADS shall undertake annual appraisal of electronic records to inform disposition. MCDAS will accordingly;

- Transfer to KNADS records selected for permanent preservation; and
- Seek approval from KNADS to destroy records recommended for disposal

7.7.6 The following disposition actions may be applicable;

- Destruction of records and metadata;
- Transfer of control of records and metadata to an organization that has assumed responsibility for the business activity through restructuring, sale, privatization or other business change;
- Transfer of electronic records and metadata to the KNADS for permanent preservation.

7.7.7 Electronic records destruction should be carried out in a way that ensures complete destruction and which complies with any security or access restrictions on the record; and be documented.

TECHNICAL COMMITTEE REPRESENTATION

The following organizations were represented on the Technical Committee:

- State Department for Culture and Heritage
- Kenya National Archives and Documentation Service (KNADS)
- Information and Communication Technology (ICT) Authority

ICT Authority
Telposta Towers, 12th Floor, Kenyatta Ave
P.O. Box 27150 - 00100 Nairobi, Kenya
t: + 254-020-2211960/62
Email: info@ict.go.ke or communications@ict.go.ke or standards@ict.go.ke
Visit: www.icta.go.ke
Become a fan: www.facebook.com/ICTAuthorityKE
Follow us on twitter: @ICTAuthorityKE


ICT
Authority