# GOVERNMENT ICT STANDARDS

# Electronic Records Management Standard

ICTA-4.002:2019

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, ICTA Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Chief Executive Officer, ICT Authority, are welcome.



## ICT AUTHORITY (ICTA)

Head Office: P.O. Box 27150, Nairobi-00100, Tel.: (+254 202) 211 960/61
E-Mail: standards@ict.go.ke, Web:http://standards.icta.go.ke

# DOCUMENT CONTROL

| | |
|---|---|
| Document Name: | Electronic Records Management Standard |
| Prepared by: | Electronic Records Management Technical Committee |
| Edition: | Second Edition |
| Approved by: | Board of Directors |
| Date Approved: | 13th January 2020 |
| Effective Date: | 1st February 2020 |
| Next Review Date: | After 3 years |

# CONTENT

# 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.

For example, 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 which are, in turn, based on the international best practices by standards development organizations including ISO.

The Authority's Directorate of Programmes and Standards has the oversight role and responsibility for management, enforcement and review of this standard. The Directorate shall carry out quarterly audits in all the Ministries, Counties, and Agencies (MCA) to determine compliance to this Standard. 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 Board who shall advise and make recommendations to remedy the shortfall.

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.

**Dr. Katherine W. Getao, EBS**

**Chief Executive Officer**

**ICT Authority**

# 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. 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 implementation of proper business information systems. Thus, there is need for strong collaboration between information and ICT professionals.

Government of Kenya public agencies will need to deploy E-records management systems to manage the vast amount of e-records that are being generated. Business information systems differ from electronic records management systems; while business information systems contain data that is commonly subject to constant updates, able to be transformed and only contain current data, electronic records management systems contain data that is not dynamically linked to business activity, unable to be altered, and may be non-current.

Generally, records management; electronic or otherwise provides a basis for:

- Enhances Consistency, accuracy, continuity and efficiency in administration and management of e-records;
- Transparent, informed and quality planning and decision-making;
- An information resource that can be used to demonstrate and account for organizational activities;
- Improving citizen access to public information and
- Maintaining the confidentiality and privacy of non-public personal information

  This standard envisages sound management of electronic records by MCDAs to ensure they have the following inherited 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 unauthorised alteration. This characteristic is also referred to as 'inviolability'.
- Usability – the record can be located, retrieved, preserved and interpreted

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.

# 1.0 SCOPE

The standard provides direction for managementof electronic records and functional requirements for E-Records Management systems.

# 2.0 Application

This Standard is applicable to

i). Central Government of Kenya
ii). County Governments
iii). State Corporations
iv). Constitutional Commissions
v). Independent Offices

# 3.0 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.

**NOTE**: KS and TR stands for Kenya Standard and Technical Report respectively.

| STANDARD CODE | TITLE OF THE STANDARD | YEAR |
|---|---|---|
| ISO 16175 | Principles and functional requirements for records in electronic office environments | 2011 |
| KS ISO/TR 12654 | Electronic imaging - Recommendations for the management of electronic recording systems for the recording of documents that may be required as evidence, on WORM optical disk. | 1997 |
| KS 2229 | Electronic records management systems - functional requirements, First Edition. | 2010 |
| KS 2374 | Electronic records management systems- Implementation guide | 2012 |

| | | |
|---|---|---|
| KS ISO 22310 | Information and documentation - Guidelines for standards drafters for stating records management requirements in standards. | 2006 |
| KS ISO 15489-1 | Information and documentation - Records management - Part 1: General. | 2016 |
| KS ISO/TR15489-2 | Information and documentation - Records management - Part 2: Guidelines. | 2001 |
| KS ISO 23081-1 | Information and documentation - Records management processes - Metadata for records - Part 1: Principles | 2017 |
| KS ISO23081-2 | Information and documentation – Managing metadata for records - Part 2: Conceptual and implementation issues. | 2009 |

## 4.0 TERMS AND DEFINITIONS

For the purpose of this Standard the following definitions, abbreviations and symbols will apply:
Access Right, opportunity, means of finding, using or retrieving information
Agent Individual, workgroup or organization responsible for, or involved in record creation, capture and/or records management processes

### 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.

### Business Classification Scheme

Tool for linking records to the context of their creation

### Business Systems

These refer to automated systems purpose built or customized that create or manage data about processes and activities of an organization. They include applications whose primary purpose is to facilitate transactions between an organizational unit and its customers, for instance a client-relationship management system.

### Classification

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

### Content

Basic data or information carried in a record; substance of the record that captures sufficient information to provide evidence of a business transaction
Context: Documents the relationship of the record to the business and technical environment in which it arises.

### Conversion

Process of changing records from one format to another

### Data Element

Specific entries under a field

### Destruction

It is the process of eliminating or deleting a record, beyond any possible reconstruction. In this standard, term destruction will refer to a disposal process whereby digital records, record plan entities and their metadata are permanently removed, erased or obliterated as authorized 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

### Document

Refer to recorded information or an object that can be treated as a unit.

### Electronic Documents

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

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

### Electronic Document Management System (EDMS):

This is an electronic system that can collect and organize documents for storage, retrieval, and tracking purpose.
Electronic document management systems are distinguished from information systems by links to activities they document and their ability to preserve and provide access to the content, structure, and context of the records.

### Electronic Document and Records Management System (EDRMS):

An electronic records management system capable of providing document management functionality.

### 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 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.

### 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 organization. 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.

### Official Record

A record that was made or received pursuant to law or in connection with the transaction of official business

### Record

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

### Record Series

This is a group of logically related records with the same retention and disposition value. An electronic record series may support one or more operations within an organization.

### 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.

### Records Management Task Force:

A group responsible for reviewing and approving records retention schedules.
The taskforce will normally include representatives from the Kenya National Archives and Documentation Services, Office of the Attorney General of Kenya, Office of the Auditor General and any other state agency as shall be determined by the Records Management Committee.

### Rendering

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

### Retrieving

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

### Redacting

The process of masking or deleting information in a record.

# 5.0 Acronyms and Abbreviations

| | |
|---|---|
| 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 |
| 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 |

## Requirements for E-Records Management

### 6.1 General

6.1.1 MCDAs shall establish a Records Management Committee

6.1.2 MCDAs shall maintain an electronic records management policy.
Note: In the development of the ERM policy, MCDAs will take into consideration;

a. Legal and regulatory requirements that must be met by the policies, procedures, and technology used to manage e-records. See Appendix 3 - ICT Governance Standard
b. Their key business operations and valuable records generated from their transactions
c. Business needs that should be addressed but can be modified or replaced when an e- records system is developed.
d. Past practices in managing paper records that can be eliminated when an ERM system is developed.

6.1.3 MCDAs shall provide training and adequate support to ensure users understand and implement ERM system procedures.

6.1.4 MCDAs shall maintain 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 shall be maintained.

6.1.5 The MCDA shall clearly define the roles and responsibilities of the human resource managing e-records and ERMS.

6.1.6 Records must be classified using the GoK classification scheme – secret, top secret, restricted, confidential

### 6.2 Capturing of e-records

6.2.1 MCDAs shall designate a receiving device(s) for e-records. This should support export, import or migration of the records.

NOTE: A "device" could mean a specific server but it also could be a specific e-mail address or website.

### 6.3 Classification and Indexing

6.3.1 MCDAs shall establish, implement and maintain a business classification scheme

6.3.2 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.

6.3.3 Indexing metadata shall be linked with records at the point of capture, and/ or added as required throughout their existence

NOTE: Examples of Indexing metadata include title, time, date, subjects, location or personal names

### 6.4 Access Control and Storage

6.4.1 MCDAs shall:

(a) Define the rights of access, permissions and restrictions as applicable
(b) Define roles and responsibilities of individuals involved in e-records creation, maintenance, and disposition
(b) Maintain physical and environmental security controls
(c) Maintain logical access control mechanisms

6.4.2 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.

6.4.3 MCDAs shall maintain problem resolution procedures including incident reporting and response procedures

NOTE: Logical controls include authentication, authorization, and accountability

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

### 6.5 Migration and Conversion

6.5.1 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.

6.5.2 The disposition of source records following a migration or conversion process shall be authorized.

6.5.3 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.

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

### 6.6 Retention and Disposal

6.6.1 MCDAs shall adopt and use records retention and disposal schedules in compliance with the laws especially;

(a) Public Archives and Documentation Service Act Cap 19
(b) Records Disposal Act Cap 14

6.6.2 MCDAs shall ensure electronic records management systems use standard formats to help reduce the rate of technological obsolescence and the need for migration

6.6.3 MCDAs shall put in place measures to ensure 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

Note: The standard formats can be relational databases, ASCII, Portable Document Format and SGML among others.

6.6.4 The following disposal action 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 restructure, sale, privatization or other business change;
- Transfer of control of records and metadata to an institutional or external archive for permanent retention.

Note: The following principles should govern the destruction of records:

(a) Destruction should always be authorized;
(b) Records pertaining to pending or actual litigation or legal action or investigation should not be destroyed while that action is underway or anticipated to arise;
(c) 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;
(d) Destruction, like any disposition action, should be documented.

### 6.7 Electronic Records Management Systems

6.7.1 E-Records Management Systems shall effectively support creation, maintenance and disposition of e-records.

6.7.2 MCDAs shall acquire ERM products and services systems in accordance with:

a) ICTGovernance and Systems and
b) Systems and Applications Standards.

6.7.3 The functional requirements of ERM systems shall be as provided in Annex A

### 6.8 Business Systems

6.8.1 All business Systems shall be able to;

a) Create, manage, maintain electronic records, and
b) Support import, export and interoperate with an e-records management system.

# ANNEXES

## Annex A: ERM System Functional Requirements

### A.1 Creation of E-Records

| | |
|---|---|
| **Record capture**<br>ERM System shall: | |
| 1 | Enable integration with business system so that transactional records created can be captured within the ERM System including electronic mails. |
| 2 | Indicate when an individual record is captured within the ERM System |
| 3 | Prevent the alteration of the content of any record by any user or administrator during the process of records capture. |
| 4 | Prevent the destruction or deletion of any record by any user, including an administrator, with the exceptions of:<br>• destruction in accordance with a disposition authority and<br>• authorized deletion by recordsadministrator |
| 5 | For default file naming systems,ERM System must allow for manual naming of electronic records at the time of capture (including email subject lines used to construct record titles). |
| 6 | Allow recordsadministrator to alter the metadata of a record within the system if required, to allow finalisation/correction of the record profile. Any such action must be captured in a records management metadata. |
| 7 | Any revision or alteration of metadata must be captured as additional records metadata. |
| 8 | Alert a user of unsuccessful capture of a record. |
| 9 | Be able (where possible and appropriate) to provide a warning of an attempt to capture a record that is incomplete or inconsistent in a way which will compromise its future apparent authenticity. |
| **Capture of Metadata**<br>ERM System shall: | |
| 10 | Support use of persistent metadata for records. |
| 11 | Acquire metadata elements for each record and persistently link them to the record over time. |
| 12 | Ensurethat the values for metadata elements conform to specified encoding schemes. |
| 13 | Allow the records administrator to pre-define (and re-define) the metadata elements associated with each record, including whether each element is mandatory or optional. |
| 14 | Allow all metadata for every record to be viewed by users, subject to access rights for individuals or groups of users. |

| | |
|---|---|
| 15 | Automatically capture the date and time of capture of each record as metadata elements linked to each record. |
| 16 | Support automatic extraction or migration of metadata from:<br>• the software application that created the record;<br>• an operating system or line of business system;<br>• an electronic records management system; and<br>• The file header, including file format metadata, of each record and its constituent components captured into the system. |
| 17 | Shall not allow for alteration of metadata captured unless authorised by the system administrator. |
| 18 | Allow entry of additional metadata by users during record capture andor a later stage of processing by the user. |
| 19 | Allow ONLY authorised users and administrators change the content of records management metadata elements. |
| 20 | Allocate an identifier, unique within the system, to each record at point of capture automatically. |
| **Aggregation**<br>ERM System shall: | |
| 21 | Ensure that all records captured within the ERM system are associated with at least one aggregation, but support the ability to assign records to multiple aggregations without their duplication |
| 22 | Manage the integrity of all markers or other reference tags to records (where used), ensuring that:<br>• following a marker, whichever aggregation that the marker record is located in, will always result in correct retrieval of the record; and<br>• Any change in location of a record also redirects any marker that references that record. |
| 23 | Not impose any practical limit on the number of records that can be captured in an aggregation, or on the number of records that can be stored in the ERM system. However, the system may permit the administrator to set limitations on the quantity of items within an aggregation if required for business purposes. |
| 24 | Allow users to choose at least one of the following where an electronic object has more than one manifestation:<br>• register all manifestations of the object as one record;<br>• register one manifestation of the object as a record; or<br>• Register each manifestation of the object as a discrete record. |

| | |
|---|---|
| **Bulk importing**<br>ERM System shall: | |
| 25 | Be able to capture in bulk, records exported from other systems, including capture of:<br>• electronic records in their existing format, without degradation of content or structure, retaining any contextual relationships between the components of any individual record;<br>• electronic records and all associated records management metadata, retaining the correct contextual relationships between individual records and their metadata attributes; and<br>• The structure of aggregations to which the records are assigned, and all associated metadata, retaining the correct relationship between records and aggregations. |
| 26 | Be able to import any directly associated event history metadata with the record and/or aggregation, retaining this securely within the imported structure. |
| **Electronic document formats**<br>ERM System shall: | |
| 27 | Support the capture of records created in native file formats from commonly used software applications such as:<br>• standard office applications (word processing, spread-sheeting, presentation, simple databases);<br>• email client applications;<br>• imaging applications;<br>• Web authoring tools. |
| 28 | Be able to extend the range of file formats supported as new file formats are introduced for business purposes or for archival retention |
| **Compound records**<br>ERM System shall: | |
| 29 | Capture compound electronic records (records comprising more than one component) so that:<br>• the relationship between the constituent components of each compound record is retained;<br>• the structural integrity of each compound record is retained; and<br>• Each compound record is retrieved, displayed and managed as a single unit. |
| 30 | Be able to capture compound records easily, preferably with one action, for example, a single click. |

| | |
|---|---|
| **Electronic mails**<br>ERM System shall: | |
| 31 | Allow users to capture emails (text and attachments) as single records as well as individual records linked by metadata. |
| 32 | Allow individual users to capture email messages (and attachments) from within their email application. |
| 33 | Allow users to choose whether to capture emails with attachments as:<br>• Email text only;<br>• Email text with attachments; or<br>• Attachments only. |
| 34 | Ensure the capture of email transmission data as metadata persistently linked to the email record. |
| 35 | Ensure that the text of an email and its transmission details cannot be amended in any way once the email has been captured. Nor should the subject line of the email itself be changeable, although the title of the record may be edited for easier access through, for example, keywords or by file-naming conventions. |
| 36 | Ensure that a human-readable version of an email message address is also captured, where one exists. |
| **Identification of Records and Associated Aggregation**<br>ERM System shall: | |
| 37 | Associate each of the following with a unique identifier:<br>• Record;<br>• Record extract; and<br>• Aggregation. |
| 38 | Require all identifiers to be unique and unduplicated within the entire ERM system. |
| 39 | Be able to store the unique identifiers as metadata elements of the entities to which they refereither by: Generating unique identifiers automatically, and prevent users from inputting the unique identifier manually and from subsequently modifying it (for example, a sequential number) |
| 40 | Allow the format of the unique identifier to be specified at configuration time. |
| 41 | Allow the administrator(s) to specify at configuration time the starting number (for example, 1, 10, 100) and increment (for example, 1, 10) to be used in all cases; this applies to automatically generated unique identifiers. |
| | **Classification Scheme**<br>ERM System shall: |
| 42 | Support and be compatible with the organisational classification scheme. |

| | |
|---|---|
| 43 | Be able to support a classification scheme that can represent aggregations (at the function, activity, transaction level) as being organised in a hierarchy with a minimum of three levels. |
| 44 | Allow the inheritance of values from a classification scheme. |
| 45 | Allow naming conventions or thesauri to be defined at the time the electronic records management system is configured. |
| 46 | Support the initial and on-going construction of a classification scheme. |
| 47 | Allow records administrators to create new aggregations at any level within any existing aggregation. |
| 48 | Not limit the number of levels in the classification scheme hierarchy unless set by records administrator. |
| 49 | Support the definition of different record types that are associated with a specified set of metadata to be applied at capture. |
| 50 | Support the allocation of unique identifiers to records within the classification structure |
| 51 | Have the capacity to automatically generate the next sequential number within the classification scheme for each new electronic aggregation (this applies to sequential unique identifiers) |
| 52 | Support browsing and graphical navigation of the aggregations and classification scheme structure, and the selection, retrieval and display of electronic aggregations and their contents through this mechanism.<br><br>NOTE:<br>The system may support a distributed classification scheme that can be maintained across a network of electronic record repositories.<br>The system may support the definition and simultaneous use of multiple classification schemes. This may be required, for example, following the merger of two organizations or migration of legacy systems. It is not intended for routine use. |
| 53 | Support metadata for levels within the classification scheme. |
| 54 | Provide at least two naming mechanisms for records in the classification scheme:<br>• a mechanism for allocating a structured alpha, numeric or alphanumeric reference code (that is, an identifier which is unique within the classification scheme) to each classification level; and<br>• A mechanism to allocate a textual title for each electronic aggregation. It must be possible to apply both identifiers separately or together. |
| 55 | Allow only authorised users to create new classifications at the highest level in the classification scheme (for example, at the business function level). |
| 56 | Record the date of opening of a new aggregation within its associated records management metadata. |
| 57 | Automatically include in the records management metadata of each new aggregation those attributes that derive from its position in the classification scheme (for example, name, and classification code). |
| 58 | Allow the automatic creation and maintenance of a list of classification levels. |

| | |
|---|---|
| 59 | Support a naming mechanism that is based on controlled vocabulary terms and relationships drawn (where appropriate) from an ISO 2788-compliant or ISO 5964-compliant thesaurus and support the linking of the thesaurus to the classification scheme. |
| 60 | Support an optional aggregation naming mechanism that includes names (for example, people's names) and/or dates (for example, dates of birth) as file names, including validation of the names against a list. |
| 61 | Support the allocation of controlled vocabulary terms compliant with ISO 2788 or ISO 5964 as records management metadata, in addition to the other requirements in this section. |
| **Classification processes**<br>ERM System shall: | |
| 62 | Allow an electronic aggregation (including volumes) to be relocated to a different position in the classification scheme, and ensure that all electronic records already allocated remain allocated to the aggregations (including volumes) being relocated. |
| 63 | Allow an electronic record to be reclassified to a different volume of an electronic aggregation. |
| 64 | Restrict to authorised users the ability to move aggregations (including volumes) and individual records |
| 65 | Keep a clear history of the location of reclassified aggregations (including volumes) prior to their reclassification, so that their entire history can be determined easily. |
| 66 | Prevent the deletion of an electronic aggregation or any part of its contents at all times, with the exceptions of:<br>• Destruction in accordance with a disposal authority; and<br>• Deletion by records administrator as part of an audited procedure. |
| 67 | Allow an electronic aggregation to be closed by a specific administrator procedure, and restrict this function to an administrator. |
| 68 | Record the date of closing of a volume in the volume's records management metadata. |
| 69 | Maintain internal integrity (relational integrity or otherwise) at all times, regardless of:<br>• Maintenance activities;<br>• Other user actions; and<br>• Failure of system components. |
| 70 | Not allow any volume that has been temporarily re-opened to remain open after the administrator who opened it has logged off. |
| 71 | Allow users to create cross-references between related aggregations or between aggregations and individual records. |
| 72 | Provide reporting tools for the provision of statistics to the administrator on aspects of activity using the classification scheme, including the numbers of electronic aggregations (including volumes) or records created, closed or deleted within a given period, by user group or functional role. |

| | |
|---|---|
| 73 | Allow the authorised users to enter the reason for the reclassification of aggregations (including volumes) and individual records. |
| 74 | Be able to close a volume of an electronic aggregation automatically on fulfilment of specified criteria to be defined at configuration, including at least:<br>• Volumes delineated by an annual cut-off date (for example, end of the calendar year, financial year or other defined annual cycle);<br>• The passage of time since a specified event (for example, the most recent addition of an electronic record to that volume); and<br>• The number of electronic records within a volume |
| 75 | Be able to open a new volume of an electronic aggregation automatically on fulfilment of specified criteria to be defined at configuration. |
| 76 | Allow system administrator to lock or freeze aggregations to prevent relocation, deletion, closure or modification when circumstances require, for example, pending legal action. |
| **Record volumes**<br>ERM Systems shall: | |
| 77 | Allow administrators to add (open) electronic volumes to any electronic aggregation that is not closed. |
| 78 | Record the date of opening of a new volume in the volume's records management metadata. |
| 79 | Automatically include in the metadata of new volumes those attributes of its parent aggregation's records management metadata that assign context (for example, name, and classification code). |
| 80 | Support the concept of open and closed volumes for electronic aggregations, as follows:<br>• Only the most recently created volume within an aggregation can be open; and<br>• All other volumes within that aggregation must be closed (subject to temporary exceptions required by Requirement 68) |
| 81 | Prevent the user from adding electronic records to a closed volume (subject to the exceptions required by Requirement 68). |
| 82 | Allow an authorised user to add records to a closed file |

### A.2 Maintenance of E-Records

| | |
|---|---|
| **Access and security**<br>ERM System shall: | |
| 83 | Ensure that records are maintained complete and unaltered, except in circumstances such as court orders for amendments to record content and metadata, in which cases only system administrators may undertake such changes with appropriate authorisation. |
| 84 | Document any exceptional changes to records as described in Requirement 88 in relevant metadata. |
| 85 | Maintain the technical, structural and relational integrity of records and metadata in the system. |
| **Access control**<br>ERM System shall: | |
| 86 | Restrict access to system functions according to a user's role and strict system administration controls |
| **Security control**<br>ERM System shall: | |
| 87 | Allow only administrators to set up user profiles and allocate users to groups. |
| 88 | Allow the administrator to limit access to records, aggregations and records management metadata to specified users or user groups. |
| 89 | Allow the administrator to alter the security category of individual records. |
| 90 | Allow changes to security attributes for groups or users (such as access rights, security level, privileges, initial password allocation and management) to be made only by the administrator. |
| **Assigning security levels**<br>ERM System shall: | |
| 91 | Allow only the administrator to attach to the user profile attributes that determine the features, records management metadata fields, records or aggregations to which the user has access. The attributes of the profile will:<br>Prohibit access to the electronic records management system without an accepted authentication mechanism attributed to the user profile;<br>• Restrict user access to specific records or aggregations;<br>• Restrict user access according to the user's security clearance;<br>• Restrict user access to particular features (for example, read, update and/or delete specific records management metadata fields);<br>• Deny access after a specified date; and<br>• Allocate the user to a group or groups. 22 |
| 92 | Be able to provide the same control functions for roles, as for users |
| 93 | Be able to set up groups of users that are associated with an aggregation |
| 94 | Allow a user to be a member of more than one group |

| | |
|---|---|
| 95 | Be able to limit users' access to parts of the list (if the ERM System maintains a list of aggregation). |
| 96 | Allow a user to stipulate which other users or groups can access records that the user is responsible for. |
| **Executing security controls**<br>ERM System shall: | |
| 97 | Allow the administrator, subject to Security categories (103-112), to alter the security category of all records within an aggregation in one operation. The electronic records management system must provide a warning if the security classifications of any records are lowered, and await confirmation before completing the operation |
| 98 | Allow the administrator to change the security category of aggregations |
| 99 | Record full details of any change to security category in the records management metadata of the record, volume or aggregation affected. |
| 100 | Provide one of the following responses (selectable at configuration time) whenever a user requests access to, or searches for, a record, volume or aggregation that they do not have the right to access:<br>• Display title and records management metadata;<br>• Display the existence of an aggregation or record (that is, display its file or record number) but not its title or other records management metadata; or<br>• Not display any record information or indicate its existence in any way. |
| 101 | Never include, in a list of full text or other search results, any record that the user does not have the right to access |
| 102 | Log all unauthorised attempts to access aggregations (and their volumes) or records in their respective unique metadata |
| **Security categories**<br>ERM System shall | |
| 103 | Allow security classifications to be assigned to records: such as Top Secret, Secret, Confidential, Restricted, Sensitive, Unclassified etc. |
| 104 | Allow security classifications to be selected and assigned at system level for:<br>• All levels of records aggregations (including volumes); and<br>• Individual records or record objects. |
| 105 | Allow access-permission security categorisation to be assigned:<br>• At group level (be able to set up group access to specific aggregations, record classes security or clearance levels);<br>• By organisational role;<br>• At user level; and<br>• In combination(s) of the above |

| | |
|---|---|
| 106 | Allow the assignment of a security category:<br>• At any level of records aggregation;<br>• After a specified time or event; and<br>• To a record type. |
| 107 | Support the automated application of a default value of 'Unclassified' to an aggregation or record not allocated any other security category. |
| 108 | Enable its security subsystem to work effectively together with general security products.<br>Be able to determine the highest security category of any record in any aggregation by means of one simple enquiry. |
| 109 | Support routine, scheduled reviews of security classifications |
| 110 | Restrict access to electronic aggregations/records that have a security classification higher than a user's security clearance. |
| 111 | Be capable of preventing an electronic aggregation from having a lower security classification than any electronic record within that aggregation. |
| **Records management process metadata**<br>ERM System shall | |
| 112 | Be capable of creating unalterable metadata of records management actions (actions to be specified by each agency) that are taken on records, aggregations or the classification scheme. The metadata should include the following records management metadata elements:<br>• Type of records management action;<br>• User initiating and/or carrying out the action; and<br>• Date and time of the action. |
| 113 | Track events, once the metadata functionality has been activated, without manual intervention, and store in the metadata information. |
| 114 | Maintain the metadata for as long as required. |
| 115 | Provide metadata of all changes made to:<br>• Electronic aggregations (including volumes);<br>• Individual electronic records; and<br>• Records management metadata associated with any of the above. |
| 116 | Document all changes made to administrative parameters (for example, changes made by the administrator to a user's access rights). |

| | |
|---|---|
| 117 | Be capable of capturing and storing in the metadata information about the following actions:<br>• Date and time of capture of all electronic records;<br>• Reclassification of an electronic record in another electronic volume;<br>• Reclassification of an electronic aggregation in the classification scheme;<br>• Any change to the disposal authority of an electronic aggregation;<br>• Any change made to any records management metadata associated with aggregations or electronic records;<br>• date and time of creation, amendment and deletion of records management metadata;<br>• Changes made to the access privileges affecting an electronic aggregation, electronic record or user;<br>• Export or transfer actions carried out on an electronic aggregation;<br>• Date and time at which a record is rendered; and<br>• Disposal actions on an electronic aggregation or record. |
| 118 | Ensure that metadata is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that this can be achieved by authorised external personnel who have little or no familiarity with the system. |
| 119 | Be able to export metadata for specified records and selected groups of records without affecting the metadata stored by the electronic records management system. |
| 120 | Be able to capture and store violations (that is, a user's attempts to access a record or aggregation, including volumes, to which they are denied access), and (where violations can validly be attempted) attempted violations of access control mechanisms. |
| 121 | Be able, at a minimum, to provide reports for actions on records and aggregations organised:<br>• By record or aggregation;<br>• By user; and<br>• In chronological sequence |
| 122 | Allow the metadata facility to be configurable by the administrator so that the functions for which information is automatically stored can be selected. The electronic records management system must ensure that this selection and all changes to it are stored in the metadata. |
| 123 | Be able to provide reports for actions on aggregations and records organised by workstation and (where technically appropriate) by network address. |
| 124 | Allow the administrator to change any user-entered records management metadata element. Information about any such change must be stored in the metadata |
| **Tracking record movement**<br>ERM System shall: | |
| 125 | Provide a tracking feature to monitor and record information about the location and movement of both electronic and non-electronic aggregations. |

| | |
|---|---|
| 126 | Record information about movements including:<br>• Unique identifier of the aggregation or record;<br>• Current location as well as a user-defined number of previous locations (locations should be user-defined);<br>• Date item sent/moved from location;<br>• Date item received at location (for transfers); and<br>• User responsible for the move (where appropriate). |
| 127 | Maintain access to the electronic record content, including the ability to render it, and maintenance of its structure and formatting over time and through generations of office application software. |
| **Management of electronic and non-electronic records**<br>ERM System shall: | |
| 128 | Be able to define in the classification scheme non-electronic aggregations and volumes, and must allow the presence of non-electronic records in these volumes to be reflected and managed in the same way as electronic records. |
| 129 | Allow both kinds of record to be managed in an integrated manner |
| 130 | Allow a non-electronic aggregation that is associated as a hybrid with an electronic aggregation to use the same title and numerical reference code, but with an added indication that it is a hybrid non-electronic aggregation. |
| 131 | Allow a different records management metadata element set to be configured for non- electronic and electronic aggregations; non-electronic aggregation records management metadata must include information on the physical location of the non-electronic aggregation. |
| 132 | Ensure that retrieval of non-electronic aggregations displays the records management metadata for both electronic and non-electronic records associated with it. |
| 133 | Include features to control and record access to non-electronic aggregations, including controls based on Security categories (103-112), which are comparable with the features for electronic aggregations. |
| 134 | Support tracking of non-electronic aggregations by the provision of request, check-out and check-in facilities that reflect the current location of the item concerned. |
| 135 | Support the printing and recognition of bar codes for non-electronic objects (for example, documents, files and other containers), or should support other tracking systems to automate the data entry for tracking the movement of such non-electronic records. |
| 136 | Support the retention and disposal protocols and routinely apply to both electronic and non-electronic elements within hybrid aggregations. |
| 137 | Ensure that a non-electronic record is allocated the same security category as an associated electronic record within a hybrid records aggregation. |

| **Disposal**<br>ERM System shall: | |
|---|---|
| 138 | Provide a function that:<br>• Specifies disposal authorities;<br>• Automates reporting and destruction actions;<br>• Disposes of compound records as a single action; and<br>• Provides integrated facilities for exporting records and records management metadata. |
| 139 | Be able to restrict the setting up and changing of disposal authorities to the administrator only. |
| 140 | Allow the administrator to define and store a set of customised standard disposal authorities. |
| 141 | Support retention periods from a minimum of one month to an indefinite period. |
| 142 | Be capable of assigning a disposal authority to any aggregation or record type |
| 143 | By default, ensure that every record in an aggregation is governed by the disposal authority(s) associated with that aggregation. |
| 144 | Include a disposal action, agency retention period and trigger in the (metadata) record for the decision for each disposal authority. |
| 145 | For each aggregation:<br>• automatically track retention periods that have been allocated to the aggregation; and<br>• Initiate the disposal process by prompting the administrator to consider and, where appropriate approve and execute, disposal action when disposal is due. |
| 146 | Allow at least the following decisions for each disposal authority:<br>• Retain indefinitely;<br>• Present for review at a future date;<br>• Destroy at a future date; and<br>• Transfer at a future date. |
| 147 | Allow retention periods for each disposal authority to be specified at a future date, with the date able to be set in at least the following ways:<br>• Passage of a given period of time after the aggregation is opened;<br>• Passage of a given period of time after the aggregation is closed;<br>• Passage of a given period of time since the most recent record has been assigned to the aggregation;<br>• Passage of a given period of time after a specific event (event to be identified in the schedule, and will be notified to the electronic records management system by the administrator, rather than being detected automatically by the electronic records management system); and<br>• Specified as 'indefinite' to indicate long-term preservation of the records. |
| 148 | Enable a disposal authority to be assigned to an aggregation that over-rides the disposal authority assigned to its 'parent' aggregation |

| | |
|---|---|
| 149 | Allow the administrator to amend any disposal authority allocated to any aggregation at any point in the life of that aggregation. |
| 150 | Allow the administrator to change the authority(s) associated with an aggregation at any time. |
| 151 | Allow the definition of sets of processing rules that can be applied as an alerting facility to specified aggregations prior to initiation of a disposal process. |
| 152 | Provide the option of allowing electronic records or aggregations that are being moved between aggregations by the administrator to have the disposal authority of the new aggregation, replacing the existing disposal authority(s) applying to these records. |
| 153 | Allow the administrator to delete aggregations, volumes and records |
| 154 | When executing disposal authorities, the electronic records management system must be able to:<br>• Produce an exception report for the administrator;<br>• Delete the entire contents of an aggregation or volume when it is deleted;<br>• Prompt the administrator to enter a reason for the action;<br>• Ensure that no items are deleted if their deletion would result in a change to another record (for example, if a document forms a part of two records – see Section 3.1.3: Aggregation of electronic records – one of which is being deleted);<br>• Inform the administrator of any links from another aggregation or record to an aggregation or volume, that is about to be deleted, and request confirmation before completing the deletion;<br>• Alert the administrators to any conflicts, for example, items that are linked to more than one disposal action involving pointers; and<br>• Maintain complete integrity of the records management metadata at all times. |
| 155 | Automatically track all retention periods specified in these disposal authorities, and initiate the disposal process once the last of all these retention dates is reached. |
| 156 | Allow the administrator to manually or automatically lock or freeze records disposition processes (freeze for litigation or legal discovery purposes, Freedom of Information purposes, etc.). |
| 157 | Record any deletion or disposal action comprehensively in the process metadata. |
| 158 | Automatically record and report all disposal actions to the administrator. |
| 159 | Support the review process by presenting electronic aggregations to be reviewed, with their records management metadata and disposal authority information, in a manner that allows the reviewer to browse the contents of the aggregation and/or records management metadata efficiently. |
| 160 | Allow the reviewer to take at least any one of the following actions for each aggregation during review:<br>• Mark the aggregation for destruction;<br>• Mark the aggregation for transfer;<br>• Mark the aggregation for indefinite hold, for example, pending litigation; and<br>• Change the disposal authority (or assign a different schedule) so that the aggregation is retained and re-reviewed at a later date, as defined in this section. |

| | |
|---|---|
| 161 | Allow the reviewer to enter comments into the aggregation's records management metadata to record the reasons for the review decisions. |
| 162 | Alert the administrator to aggregations due for disposal before implementing disposal actions, and on confirmation from the administrator must be capable of initiating the disposal actions specified in this section. |
| 163 | Store in the metadata all decisions taken by the reviewer during reviews. |
| 164 | Produce a disposal authority report for the administrator that identifies all disposal authorities that are due to be applied in a specified time period, and provide quantitative reports on the quantity and types of records covered. |
| 165 | Be able to specify the frequency of a disposal authority report, the information reported and highlight exceptions such as overdue disposal. |
| 166 | Alert the administrator if an electronic aggregation that is due for destruction is referred to in a link from another aggregation and pause the destruction process to allow the following remedial action to be taken:<br>• Confirmation by the administrator to proceed with or cancel the process; and<br>• Generation of a report detailing the aggregation or record(s) concerned and all references or links for which it is a destination. |
| 167 | Support reporting and analysis tools for the management of retention and disposal authorities by the administrator, including the ability to:<br>• List all disposal authorities;<br>• List all electronic aggregations to which a specified disposal authority is assigned;<br>• List the disposal authority(s) applied to all aggregations below a specified point in the hierarchy of the classification scheme;<br>• Identify, compare and review disposal authorities (including their contents) across the classification scheme; and<br>• Identify formal contradictions in disposal authorities across the classification scheme. |
| 168 | Provide, or support the ability to interface with, a workflow facility to support the scheduling, review and export/transfer process by tracking:<br>• Progress/status of the review, such as awaiting or in-progress, details of reviewer and date;<br>• Records awaiting disposal as a result of a review decision; and<br>• Progress of the transfer process. |
| 169 | Be able to accumulate statistics of review decisions in a given period and provide tabular and graphic reports on the activity. |

| **Migration, export and destruction**<br>ERM System shall: | |
|---|---|
| 170 | Provide a well-managed process to transfer records to another system or to a third party organisation and support migration processes. |
| 171 | Include all aggregations, volumes, records and associated metadata within aggregations whenever an electronic records management system transfers any aggregation or volume. |
| 172 | Be able to transfer or export an aggregation (at any level) in one sequence of operations so that:<br>• The content and structure of its electronic records are not degraded;<br>• All components of an electronic record (when the record consists of more than one component) are exported as an integral unit including any technical protection measures;<br>• All links between the record and its records management metadata are retained; and<br>• All links between electronic records, volumes and aggregations are retained. |
| 173 | Be able to include a copy of the entire metadata set associated with the records and aggregations that are transferred or exported from an electronic records management system. |
| 174 | Produce a report detailing any failure during a transfer, export or destruction. The report must identify any records destined for transfer that have generated processing errors, and any aggregations or records that are not successfully transferred, exported or destroyed. |
| 175 | Retain copies of all electronic aggregations and their records that have been transferred, at least until such time as a successful transfer is confirmed. |
| 176 | Be able to continue to manage records and aggregations that have been exported from the electronic records management system to other forms of storage media. |
| 177 | Have the ability to retain records management metadata for records and aggregations that have been destroyed or transferred. |
| 178 | Allow the administrator to specify a subset of aggregation records management metadata that will be retained for aggregations which are destroyed, transferred out or moved offline. |
| 179 | Enable the total destruction of records (whether identified by class or individually) stored on re-writable media by completely obliterating them so that they cannot be restored through specialist data recovery facilities. |
| 180 | Provide a utility or conversion tool to support the conversion of records marked for transfer or export into a specified file transfer or export format. |
| 181 | Provide the ability to add user-defined records management metadata elements required for archival management purposes to electronic aggregations selected for transfer. |
| 182 | Provide the ability to sort electronic aggregations selected for transfer into ordered lists according to user-selected records management metadata elements. |

| | |
|---|---|
| 183 | Require the administrator to confirm that the non-electronic part of the same aggregations has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part. |
| | **Retention and disposal of electronic and non-electronic records** |
| | ERM System shall: |
| 184 | Support the allocation of disposal authorities to every non-electronic aggregation in the classification scheme. The authorities must function consistently for electronic and non- electronic aggregations, notifying the administrator when the disposal date is reached, but taking account of the different processes for disposing of electronic and non- electronic records. |
| 185 | Support the application of the same disposal authority to both the electronic and non-electronic aggregations that make up a hybrid aggregation. |
| 186 | Be able to apply any review decision made on a hybrid electronic aggregation to a non-electronic aggregation with which it is associated. |
| 187 | Alert the administrator to the existence and location of any hybrid non-electronic aggregation associated with a hybrid electronic aggregation that is to be exported or transferred. |
| 188 | Be able to record in the metadata all changes made to records management metadata references to non-electronic or hybrid aggregations and records. |
| 189 | Be capable of offering check-out and check-in facilities for non-electronic aggregations profiled in the system, in particular enabling the ability to record a specific user or location to which a non-electronic aggregation is checked out, and to display this information if the non-electronic aggregation is requested by another user. |
| 190 | Be capable of offering a request facility for non-electronic records profiled in the hybrid aggregation system, enabling a user to enter a date that the non-electronic element is required and generating a consequent message for transmission to the current holder of that non-electronic aggregation or the administrator, according to configuration. |
| 191 | Be able to export and transfer records management metadata of non-electronic records and aggregations. |
| 192 | Support the application of a review decision taken on a group of aggregations to any non-electronic aggregations within that group, by notifying the administrator of necessary actions to be taken on the non-electronic aggregations. |

### A.3 Dissemination of E-Records

| | **Search and retrieval**<br>ERM System shall: |
|---|---|
| 193 | Provide a flexible range of functions that operate on the metadata related to every level of aggregation and on the contents of the records through user-defined parameters for the purpose of locating, accessing and retrieving individual records or groups of records and/or metadata. |
| 194 | Allow all record, volume and aggregation records management metadata to be searchable. |
| 195 | Allow the text contents of records (where they exist) to be searchable |
| 196 | Allow the user to set up a single search request with combinations of records management metadata and/or record content. |
| 197 | Allow administrators to configure and change the search fields to:<br>• Specify any element of record, volume and aggregation records management metadata, and optionally full record content, as search fields; and<br>• Change the search field configuration. |
| 198 | Provide searching tools for:<br>• Free-text searching of combinations of record and aggregation records management metadata elements and record content; and<br>• Boolean searching of records management metadata elements (see also Requirement 219). |
| 199 | Provide for 'wild card' searching of records management metadata that allows for forward, backward and embedded expansion. |
| 200 | Allow searching within a single aggregation or across more than one aggregation. |
| 201 | Be able to search for, retrieve and display all the records and records management metadata relating to an electronic aggregation, or volume, as a single unit. |
| 202 | Be able to search for, retrieve and render an electronic aggregation by all implemented naming principles, including:<br>• Name; and<br>• Identifier (classification code). |
| 203 | Display the total number of search results on a user's screen and must allow the user to then display the results list, or refine the search criteria and issue another request. |
| 204 | Allow records and aggregations featured in the search results list to be selected, then opened (subject to access controls) by a single click or keystroke. |
| 205 | Allow users to retrieve aggregations and records directly through the use of a unique identifier. |
| 206 | Never allow a search or retrieval function to reveal to a user any information (records management metadata or record content) that the access and security settings are intended to hide from that user. |

| | |
|---|---|
| 207 | Have integrated search facilities for all levels of the classification scheme |
| 208 | Provide free-text and records management metadata searches in an integrated and consistent manner. |
| 209 | Present seamless functionality when searching across electronic, non-electronic and hybrid aggregations. |
| 210 | Allow users to save and re-use queries. |
| 211 | Allow users who are viewing or working with a record or aggregation, whether as the result of a search or otherwise, to see the record within the classification or aggregation hierarchy easily and without leaving or closing the record. |
| 212 | Allow users to refine (that is, narrow) searches |
| 213 | Provide a browsing mechanism that enables graphical or other display browsing techniques at any level of aggregation (this applies to where a graphical user interface is employed) |
| **Rendering: displaying records**<br>ERM System shall: | |
| 214 | Render or download records that the search request has retrieved |
| 215 | Render records that the search request has retrieved without loading the associated application software |
| 216 | Be able to render all the types of electronic records specified by the organisation in a manner that preserves the information in the records (for example, all the features of visual presentation and layout produced by the generating application package), and which renders all components of an electronic record in their original relationship |
| **Rendering: printing**<br>ERM System shall: | |
| 217 | Provide the user with flexible options for printing records and their relevant records management metadata, including the ability to print a record(s) with records management metadata specified by the user. |
| 218 | Allow the printing of records management metadata for an aggregation. |
| 219 | Allow the user to be able to print out a summary list of selected records (for example, the contents of an aggregation), consisting of a user-specified subset of records management metadata elements (for example, Title, Author, Creation date) for each record. |
| 220 | Allow the user to print the results list from all searches. |
| 221 | Be able to print all the types of electronic records specified by the organisation. Printing must preserve the layout produced by the generating application package(s) and include all (printable) components of the electronic record. |
| 222 | Allow the administrator to specify that all printouts of records have selected records management metadata elements appended to them, for example, title, registration number, and date and security category. |

| | |
|---|---|
| 223 | Allow the administrator to print:<br>• The thesaurus, where a thesaurus exists within the system.<br>• Any and all administrative parameters<br>• Disposition authorities<br>• The classification scheme<br>• Metadata schema or element sets<br>• The file list.( If the electronic records management system uses classification schemes and thesauri) |
| 224 | Allow all records in an aggregation to be printed, in the sequence specified by the user, in one operation. |
| **Rendering: redacting records**<br>ERM System shall: | |
| 225 | Allow the administrator to take a copy of a record for the purposes of redaction. |
| 226 | Record the creation of extracts in the records management metadata, including at least date, time, reason for creation and creator. |
| 227 | Store in the metadata any change made in response to the requirements in this section. |
| 228 | Provide functionality for redacting (see Glossary at Appendix A) sensitive information from the extract. If the electronic records management system does not directly provide these facilities, it must allow for other software packages to do so. |
| 229 | Prompt the creator of an extract to assign it to an aggregation. |
| 230 | Store a cross-reference to an extract in the same aggregation and volume as the original record, even if that volume is closed. |
| **Rendering: non - printable records**<br>ERM System shall: | |
| 231 | Include features for rendering those records that cannot be meaningfully printed (for example audio, visual and database files)to an appropriate output device |
| **Rendering: Re-purposing content**<br>ERM System shall: | |
| 232 | Allow the re-use or re-purposing of content. |

## A.4. ADMINISTRATION OF E-RECORDS

| | |
|---|---|
| **Administrator Functions**<br>ERM System shall: | |
| 233 | Allow the system administrator to retrieve, display and re-configure system parameters and to re-allocate users and functions between user roles. |
| 234 | Provide back-up facilities so that records and their records management metadata can be recreated using a combination of restored back-ups and metadata. |
| 235 | Provide recovery and rollback facilities in the case of system failure or update error, and must notify the administrator of the results |
| 236 | Monitor available storage space and notify the administrator when action is needed because available space is at a low level or because it needs other administrative attention. |
| 237 | Allow the records administrator to make bulk changes to the classification scheme, ensuring all records management metadata and metadata data are handled correctly and completely at all times, in order to make the following kinds of organisational change:<br>• Division of an organisational unit into two;<br>• Combination of two organisational units into one;<br>• Movement or re-naming of an organisational unit; and<br>• Division of a whole organisation into two organisations |
| 238 | Support the movement of users between organisational units. |
| 239 | Allow the definition of user roles, and must allow several users to be associated with each role. |
| 240 | Communicate any errors encountered in saving data to storage media. |
| **Metadata administration**<br>ERM System shall: | |
| 241 | Allow the records administrator to;<br>• Create, define and delete metadata elements, including custom fields.<br>• Apply and modify metadata schema rules, including semantic and syntactical rules, encoding schemes and obligation status. |

| | |
|---|---|
| 242 | Allow the system administrator to configure the system to restrict the viewing or modifying of metadata elements by group, functional role or user. |
| 243 | Document all metadata administration activities |
| **Reporting**<br>ERM System shall: | |
| 244 | Provide flexible reporting facilities for the records administrator. They must include, at a minimum, the ability to report the following:<br>• Numbers of aggregations, volumes and records;<br>• Transaction statistics for aggregations, volumes and records; and<br>• Activity reports for individual users. |
| 245 | Allow the records administrator to report on metadata based on selected:<br>• Aggregations;<br>• Volumes;<br>• Record objects;<br>• Users;<br>• Time periods; and<br>• File formats and instances of each format. |
| 246 | Be able to produce a report listing aggregations, structured to reflect the classification scheme, for all or part of the classification scheme. |
| 247 | Allow the records administrator to request regular periodic reports and one-off reports. |
| 248 | Allow the records administrator to report on metadata based on selected:<br>• Security categories;<br>• User groups; and<br>• Other records management metadata. |
| 249 | Include features for sorting and selecting report information |
| 250 | Include features for totalling and summarising report information. |
| 251 | Allow the system administrator to restrict users' access to selected reports. |
| **Back-up and recovery**<br>ERM System shall: | |
| 252 | Provide automated back-up and recovery procedures. |
| 253 | Allow the system administrator to schedule back-up routines by:<br>• Specifying the frequency of back-up; and<br>• Allocating storage media, system or location for the back-up (for example, offline storage, separate system, remote site). |
| 254 | Allow only the administrator to restore from electronic records management system back-ups. Full integrity of the data must be maintained after restoration. |
| 255 | Allow only the administrator to roll-forward the electronic records management system from a back-up to a more recent state, maintaining full integrity of the data. |

| | |
|---|---|
| 256 | Allow users to indicate that selected records are considered to be 'vital records' |
| 257 | Be able to notify users whose updates may have been incompletely recovered, when they next use the system, that a potentially incomplete recovery has been executed. |

## ANNEX B: RECORDS MANAGEMENT COMMITTEE

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

Advice the Accounting Officer on information and records management matters
Ensure awareness, training, adoption and implementation of the ERM Standard
Ensure development and implementation of information and records management policy, procedures and guidelines.

This committee shall oversee the management of records in an MCDA.
The committee shall ensure that annual surveys and audits to determine the state of records management in the MCDA.

Also, the committee will be responsible of constituting any Task Force and or ad hoc committee herein mentioned.

The Committee shall have representation from ICT, Records, Finance, Administration and Supply Chain departments. Committee meetings will be convened at least once every quarter.
The Committee shall interface with other relevant committees
Shall have quarterly meetings and not less than 4 in a financial year.

## APPENDIX I

## CONFORMITY ASSESMENT CHECKLIST

| Sub Topic | Details | Rating | | |
|---|---|---|---|---|
| | | YES | NO | % |
| 6.1 General | 6.1.2 MCDA maintains an electronic records management policy. | | | |
| | 6.1.3 MCDA provides training and adequate support to ensure users understand and implement ERM system procedures | | | |
| | 6.1.4 MCDA 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 MCDA clearly defines the roles and responsibilities of the human resource managing e-records and ERMS. | | | |
| | 6.1.6 Records are classified using the GoK classification scheme – secret, top secret, restricted, confidential | | | |
| **6.2 Capturing of e-records** | 6.2.1 MCDA designates a receiving device(s) for e-records. This supports export, import or migration of the records. | | | |
| | 6.2.1 MCDA designates a receiving device(s) for e-records. This supports export, import or migration of the records. | | | |
| **6.3 Classification and Indexing** | 6.3.1 MCDA 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 MCDA has:<br>(a) Defined the rights of access, permissions and restrictions as applicable<br>(a) Defined roles and responsibilities of individuals involved in e-records creation, maintenance, and disposition<br>(b) Maintained physical and environmental security controls<br>(c) Maintained logical access control mechanisms | | | |
| | 6.4.2 MCDA has deployed ERM 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 MCDA has maintained problem resolution procedures including incident reporting and response procedures | | | |
| | 6.4.5 MCDA has maintained contingency plan that has include but not limited to data backup, disaster recovery and business continuity | | | |

| | | | | |
|---|---|---|---|---|
| **6.5 Migration and Conversion** | 6.5.1 MCDA 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 (digitization), to internal and external stakeholders. | | | |
| | 6.5.2 The disposition of source records following a migration or conversion process is authorized. | | | |
| | 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, authorized or certified by an ad-hoc committee (that may include internal and external stakeholders). | | | |
| **6.6 Retention and Disposal** | 6.6.1 MCDA has adopted and use records retention and disposal schedules in compliance with the laws especially;<br>(a) Public Archives and Documentation Service Act Cap 19<br>(b) Records Disposal Act Cap 14 | | | |
| | 6.6.2 MCDA ensures that electronic records management systems use standard formats to help reduce the rate of technological obsolescence and the need for migration | | | |
| | 6.6.3 MCDA has put in place measures to ensure continued usability of e-records during their retention period. These measures may include:<br>(a) Applying and maintaining appropriate and persistent metadata about a record's technical dependencies;<br>(b) Additional copies of records or converting them into alternative formats;<br>(c) Migrating records;<br>(d) Retain documented information on routine monitoring of storage conditions | | | |

| | | | | |
|---|---|---|---|---|
| | 6.6.4 The following disposal action may be applicable;<br>• Destruction of records and metadata;<br>• Transfer of control of records and metadata to an organization that has assumed responsibility for the business activity through restructure, sale, privatization or other business change;<br>• Transfer of control of records and metadata to an institutional or external archive for permanent retention. | | | |
| **6.7 Electronic Records Management Systems** | 6.7.1 E-Records Management Systems effectively supports creation, maintenance and disposition of e-records. | | | |
| | 6.7.2 MCDA has acquired ERM products and services systems in accordance with:<br><br>a) ICT Governance and Systems and<br>b) Systems and Applications Standards. | | | |
| | 6.7.3 The functional requirements of ERM systems have been as provided in Annex A | | | |
| **6.8 Business Systems** | 6.8.1 All business Systems are able to;<br><br>a) Create, manage, maintain electronic records, and<br>b) Support import, export and interoperate with an e-records management system. | | | |

| ELECTRONIC RECORDS MANAGEMENT STANDARD WORK GROUP |
| --- |
| MOSES KIJUGU- ICTA |
| JANE OTOKO- MINISTRY OF HEALTH |
| ELIZABETH MULI- KEMSA |

**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