CAPITAL MARKETS AUTHORITY

Promoting the Integrity and Growth of the Capital Markets

RECORDS MANAGEMENT AND RETENTION POLICY

RESEARCH, ANALYTICS & KNOWLEDGE MANAGEMENT DEPARTMENT

October 2025

Contents

1.Purpose

1.1 The Authority has set up an initiative to manage its records in a well-structured record keeping system and to put the necessary policies and procedures in place to ensure that its record keeping and records management practices comply with the industry's standards and the related legislation.

1.2 Information as a resource is of the same importance to good management as other standard resources like people, money and facilities. The information resources of the Authority must therefore be managed as a valuable asset. Appropriate records management is a vital aspect of maintaining and enhancing the value of this asset. The Authority considers its records to be a valuable asset to:

- Enable the Authority to find the right information easily and comprehensively.
- Enable the Authority to perform its functions successfully and efficiently and in an accountable manner.
- Support the business, legal and accountability requirements of the Authority.
- Ensure the conduct of business in an orderly, efficient and accountable manner.
- Ensure the consistent delivery of services.
- Support and document policy formation and administrative decision-making.
- Provide continuity in the event of a disaster.
- Protect the interests of the Authority and the rights of employees, clients and present and future stakeholders.
- Support and document the Authority's activities, development and achievements.
- Prevent unauthorized or unlawful disclosure of information by ensuring records are held securely and access is controlled and managed

1.3 Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater co-ordination of information and storage systems.

1.4 To measure performance and improvement, the Authority will use the national standard for records management, (Kenya National Archives and Documentation Service (KNADS) and international standards ISO 9001:2008 clause 4.2.4.

2. Definitions

- Classification: The systematic identification and arrangement of business activities and / or records into categories according to logically structured rules.
- Conversion: The process of changing records from one medium or format to another.
- Document: Recorded information or object which can be treated as a discrete unit.
- Migration: The act of moving records from one system to another, while maintaining their authenticity, integrity, reliability and usability.
- Preservation: Processes and operations used in ensuring the technical and intellectual survival of authentic records over time.
- Records: Information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.
- Records management: The efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.
- Records system: An information system which captures, manages and provides access to records through time.
- Migration: The act of moving records from one system to another, while maintaining their authenticity, integrity, reliability and usability.
- Records Conversion: The process of changing records from one medium or format to another.
- Records Storage – Preservation measures for keeping records under defined conditions and permitting their retrieval or the information contained in them.

3. Policy Statement

3.1 All records created and received at the Authority shall be managed in accordance with the records management principles contained in this policy and the guidelines on handling correspondence and mail in the Authority.

3.2 The following broad principles apply to the record keeping and records management practices at the Authority:

- The Authority follows sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.
- The records management procedures of the Authority comply with legal requirements, including those for the provision of evidence.
- The Authority follows sound procedures for the security, privacy and confidentiality of its records.
- Electronic records at the Authority are managed according to the principles and guidelines promoted by the standard's best practices and Kenya National Archives and Documentation Service Act.
- The Authority has performance measures for all records management functions and reviews compliance with these measures.

4.Scope and Intended Audience

4.1 This policy impacts upon the Authority's work practices for all those who:

- Create records including electronic records.
- Have access to records.
- Have any other responsibilities for records, for example storage and maintenance responsibilities.
- Have management responsibility for staff engaged in any of these activities; or manage, or have design input into, information technology infrastructure.

4.2 The policy therefore applies to all staff members of the Authority and covers all records regardless of format, medium or age.

5. Regulatory Framework

5.1 By managing its paper-based and electronic records effectively and efficiently the Authority strives to have effect on the accountability, transparency and service delivery values contained in the legal framework. References made to:

- The Constitution of Kenya 2010
- The Kenya Information and Communications Act, Chapter 411A
- The CMA ICT and ICT Security Policy
- The ISO 9001:2008 standards-Control of Records
- Kenya National Archives and Documentation Service Act 19
- Data Protection Act 2019 and The Data Protection (General) Regulations, 2021.
- ISO 15489 international standards for
- And any other related legislation as they may come into force

6.Record Management Systems

6.1 Each department must have in place adequate systems for documenting its principal activities and ensuring that it creates and maintains records possessing ‘authenticity, reliability, integrity and usability.

6.2 There must be a clear allocation of responsibility within each department for all aspects of record-keeping, including classifying documents and secure disposal. The ownership of information must also be clarified, so that there is no ambiguity regarding responsibility for its maintenance and disposal. Shared drives, mailing lists and role accounts should be used as a default.

6.3 Line managers must ensure that when a staff member leaves the organization, all records and information stored on personal drives or in locations not accessible to colleagues are identified and appropriately transferred to another designated staff member. In addition, any information that is no longer relevant or required should be securely deleted to maintain data integrity and prevent unnecessary retention.

6.4 Records systems must be adequately documented, so that their effective operation does not depend on the memory of individual members of staff. They should also be periodically reviewed, and modified where necessary, to ensure that they continue to support local needs. In particular, electronic systems storing data that may be required for evidential purposes should be regularly monitored and audited: it must be possible to demonstrate the reliability of the system, so that the integrity of the data cannot be questioned.

6.5 File/Document Management, Movement of files and documents shall be controlled either manually by use of file movement registers or through a records management information system (CRM).

6.6 Records shall be maintained and controlled to ensure adequate storage and protection in order to enhance accuracy and authenticity. This shall entail: -

- Developing registry procedure manual
- Preparation and use of appropriate filing classification and indexing schemes
- Preparation and use of sound records retention and disposal schedule
- Provision of registry rooms for management of current and semi-current records.
- Provision of records centres in all of the department's housing and servicing of semi-current records
- Provision of modern equipment and facilities for storage and preservation of records.
- Establishing the Authority archive for housing and preservation of valuable records.
- Enhanced use of ICT for management of records.
- Putting in place disaster plan and recovery programme.

7 Creating Records

7.1 Records must be accurate and complete, so that it is possible to establish what decisions and actions have been taken, and why. The quality of the records must allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met.

7.2 Information should be compiled at the time of the event or transaction to which it relates, or as soon as possible afterwards, and protected from unauthorized alteration or deletion. Where relevant, templates should be used, so that documents are produced consistently and quickly.

7.3 Standardized referencing and titling are essential, so that information can be promptly identified and retrieved. Naming conventions and glossaries should be used to ensure the consistent use of terms. Version control is also required for the drafting and revision of documents, so that different versions can be distinguished and the latest version readily identified.

8 Classification

8.1 All records, whether paper or electronic, must be organized logically, so that they can be easily and speedily retrieved. A classification scheme or filing structure should be devised, based on an analysis of a department's functions and activities, to ensure that documents are organized appropriately and consistently. Similar records should be grouped together.

9 Roles and Responsibilities

9.1 Directorate of Technology Research and Knowledge Managemen*t* (DTRKM)

9.1.1 DTRKM will be charged with the responsibility of overseeing the records management policy implementation by the Authority

9.1.2 DTRKM is committed to enhancing accountability, transparency and improvement of service delivery by ensuring that sound records management practices are implemented and maintained.

9.1.3 DTRKM supports the implementation of this policy and requires each staff member to support the values underlying in this policy.

9.1.4 DTRKM shall designate an Officer to perform such duties as are necessary to enhance the record keeping and records management practices of the Authority to the principles and guidelines listed in this document and to enable compliance with legislative and regulatory requirements.

9.2 Departmental/Unit Managers

9.2.1 Directorate / Departmental /Unit Managers are responsible for the implementation of this policy in their respective units.

9.2.2 Directorate / Departmental /Unit Managers are responsible for defining record classification structure in their respective units.

9.2.3 Directorate / Departmental /Unit Managers are responsible for defining access control matrix for records maintained in their sections.

9.2.4 Directorate / Departmental /Unit Managers shall ensure that all records and documents maintained by their sections are filed centrally and not in personal files/folders

9.2.5 Directorate / Departmental/Unit Managers shall lead by example and shall themselves maintain good record keeping and records management practices.

9.2.6 Senior Management shall ensure that staff are informed of their responsibilities and obligations regarding recordkeeping and records management.

9.2.7 Directorate/Departmental/unit Managers shall ensure that the management of records including e-mail and e-records are key responsibilities in the performance agreements of all the staff in their units. All scanned and e-mail records should be arranged/managed in similar criteria used in managing records in shared drives i.e. using folders

9.3 ICT Department

The department shall:

9.3.1 Be responsible for the day-to-day maintenance of electronic systems that store records.

9.3.2 Work in conjunction with the records officer / registry staff to ensure that records are properly managed, protected and appropriately preserved for as long as they are required for business, legal and long-term preservation purposes.

9.3.3 Ensure that all electronic systems capture appropriate systems generated metadata and audit trail data for all electronic records to ensure that authentic and reliable records are created.

9.3.4 Ensure that electronic records in all electronic systems remain accessible by migrating them to new hardware and software platforms when there is a danger of technology obsolescence including media and format obsolescence.

9.3.5 Ensure that all data, metadata, audit trail data, operating systems and application software are backed up on a daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible records should a disaster occur.

9.3.6 Ensure that back-ups are stored in a secure off-site environment.

9.3.7 Ensure that systems that manage and store records are virus free.

9.3.8 Ensure all shared electronic records are protected by the appropriate access controls to maintain data confidentiality, integrity and authorized use

9.3.9 Support physical security by managing access controls systems for registry doors to ensure only authorized personnel have access to secure aeras.

9.4 Registry staff

9.4.1 The registry staff will be responsible for the physical management of the records in their care.

9.4.2 Detailed responsibilities regarding the day-to-day management of the records in the registry are contained in the Registry Procedure Manual.

9.5 Staff

9.5.1 Every staff member shall create records of transactions while conducting official business.

9.5.2 Every staff member shall manage those records efficiently and effectively by:

- Filing all electronic records in a defined central location.
- Allocating reference numbers and subjects to paper-based and electronic records according to the registry file classification scheme.
- Sending paper-based records to the registry for filing.
- Ensuring that records are destroyed/deleted only in accordance with the Kenya Information and Communications Act, Chapter 411 A.

9.5.3 Records management responsibilities shall be written into the performance agreements of all staff members to ensure that staff are evaluated on their record management responsibilities.

10. Registries

10.1 Executive Registry/Main Registry

10.1.1 The Authority shall maintain two registries for confidential and general purposes. The two registries may or may not be in different locations, however they shall provide easy standard, storage, access, indexing and retrieval of all available records within reasonable timeframes.

10.1.2 All paper-based correspondence records that are not confidential are housed in the Main registry.

10.1.3 All confidential records and staff personal files will be housed in the Executive registry.

10.1.4 All these records are under the management of the registry staff who are mandated to ensure that they are managed properly.

10.1.5 The registry is a secure storage area and only registry staff are allowed in the records storage area.

10.1.6 Staff members that need access to files in the registry shall place a request for the files at the counter.

10.1.7 The registry shall remain locked and secured at all times when it is not in operation.

11 Electronic Records

11.1 The Authority shall generate and manage various records in the form of computer files and electronic correspondence, which shall be stored either in designated personal folders or in shared folders on the server, in accordance with established data management and access control policies.

11.2 The files will be backed up daily to an off-site location.

11.3 The workflow system (CRM) shall be used as an electronic equivalent of the registry.

11.4 This system also stores the approval chain of the documents allowing knowledge of who approved any document.

11.5 Detailed guidance regarding the management of these systems shall be as contained in the ICT policy.

11.6 The Authority shall implement and maintain electronic records for procurement requisitions, store requisitions, leave workflows, and other documentation related to business processes through an integrated workflow management system.

12.0 E-mails as Records

12.0.2 E-mails that are evidence of the business transactions of the Authority are public records and shall be managed and kept for as long as they are required for functional and/or historical purposes.

12.0.3 E-mails that approve an action, authorize an action, contain guidance, advice or direction, relate to projects and activities being undertaken, and external stakeholders, represent formal business communication between staff, contain policy decisions, etc. should be managed as records and should be arranged in a record-keeping system.

12.0.4 This policy covers the e-mail message itself as well as any attachments that meet these criteria.

12.1 An e-mail message is a record if it:

12.0.5 Contains unique, valuable information developed in preparing board/CNF papers, reports, publications .

12.0.6 Reflects significant actions taken in the course of conducting business.

12.0.7 Conveys unique, valuable information about the Authority's programs, policies, decisions, or essential actions.

12.0.8 Conveys statements of policy or the rationale for decisions or actions.

12.0.9 Documents oral exchanges (in person or by telephone), during which policy is formulated, or other business activities are planned or transacted.

12.0.10 Adds to the proper understanding of the formulation or execution of the Authority's actions or of operations and responsibilities.

12.0.11 Documents important meetings.

12.0.12 Facilitate action by the Authority's officials and their successors in office.

12.0.13 Protects the financial, legal, and other rights of the Authority and of the people directly affected by the Authority's actions.

12.0.14 Approves or authorizes actions or expenditure.

12.0.15 Constitutes formal communication between staff e.g. correspondence or memoranda relating to official business.

12.0.16 Signifies a policy change or development.

12.0.17 Creates a precedent e.g. by issuing instructions or advice.

12.0.18 Involves negotiations on behalf of the Authority.

12.1 E-mails that contain the following do not need to be filed:

12.2.1 Meeting announcements.

12.2.2 Announcements of employees' absences or schedules.

12.2.3 Changes in telephone numbers or office locations.

12.2.4 Meeting arrangements that normally would have been done by telephone.

12.2.5 Copies of memoranda or text sent for information rather than action.

12.2.6 Messages that have only temporary value such as a message that a meeting time has changed.

12.2.7 Duplicate information already documented in existing records.

13. Records Retention

13.1 Records should be kept as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests.

13.2 Records must only be kept for as long as they are required to meet operational, business and legal needs. As established by the Data Protection Act.

13.3 The Authority needs to have clearly defined procedures for the retention and disposal of records, to demonstrate corporate responsibility in the management of its information and records.

13.4 Files should be reviewed regularly to ensure records are not kept for too long. If there is no alternative, the entire file should be retained for the longest relevant retention period.

13.5 Line managers are responsible for ensuring that the retention periods are regularly reviewed to determine whether any retention periods applying to information within their department have expired. Once the retention period has expired, relevant action must be taken.

14.Disposal of Records

14.1 Records should be reviewed regularly, and any temporary or unnecessary items, such as draft copies, routine emails, outdated reference material, or duplicate documents should be removed. This helps prevent clutter and ensures that only important and official records take up storage space.

14.2 Disposal of records, both paper and electronic, is controlled by the retention schedule and carried out by authorized staff. When the retention period expires, all copies should be destroyed, wherever they are held.

14.3 Destruction should also be documented, to provide evidence that retention schedules have been followed and to prevent searching for material that no longer exists.

14.4 Records shall be destroyed/ deleted only in accordance with the written disposal authority issued by the Kenya National Archivist and Documentation Services.

15 Training and Awareness

15.1 The Authority should ensure that all staff are trained on the efficient usage of the email system and workflow system as well as the registry functions of the Authority.

16. Policy conflict with Legislation

16.1 Where this policy conflicts with any piece of legislation, the Law will take precedence over the policy.

17.Review of the Policy

17.1 The policy shall be reviewed from time to time on need basis in order to reflect changing business and technology.