CERTIFICATION RECORD CONTROL PROCEDURE

ICTA-DPS-PRC-001

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

REVISION HISTORY

Revision/Version	Date of change	Description of Change	Approver details

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:	Certification Record Control Procedure
Prepared by:	Deputy Director Standards and Processes
Edition:	First Edition
Approved by:	Director Programmes and Standards
Date Approved:	1st March 2025
Effective Date:	1st March 2025

CONTENTS

1.0 PURPOSE

This procedure defines the scheme for the identification, storage, protection, retrieval, retention, and disposal of records associated with the ICT Authority's certification activities. It ensures that all records:

i. Support certification decisions and traceability.
ii. Are securely stored and maintained in compliance with ISO/IEC 17024 and legal requirements.
iii. Are disposed of securely to prevent unauthorized access or misuse.

2.0 SCOPE

This procedure applies to all certification-related records, including:

i. Certification applications and supporting documents.
ii. Assessment and evaluation reports.
iii. Certification decisions and client correspondence.
iv. Inactive or expired certification records.

3.0 DEFINITION

Term	Definition
Client Records	Documentation related to individuals or organizations seeking or holding certification
Retention Period	The time frame for which records must be maintained before disposal.
Controlled Document	A document that is formally managed to ensure compliance and consistency
Secure Storage:	Protection measures, including encryption, restricted access, and backups

4.0 ROLES & RESPONSIBILITIES

Term	Definition
Records Officer	• Manages and maintains records throughout their lifecycle. • Ensures proper classification, storage, and retrieval of records. • Implements security measures for physical records. • Processes disposal requests and maintains disposal logs.
Certification Manager	• Approves access to confidential or restricted records. • Establishes retention policies for certification-related records. • Reviews and authorizes the final disposal of sensitive records. • Ensures compliance with regulatory and accreditation requirements.

Term	Definition
Auditors/Internal Quality Assurance	• Conducts regular audits to verify compliance with ISO/IEC 17024. • Ensures retrieval, protection, and disposal procedures meet security and regulatory requirements. • Reviews records classification, storage, and retention processes. • Recommends improvements to enhance compliance and security.

5.0 PROCEDURES

5.1 Records Identification Process

5.1.1 Categories of Records for Certification Activities

5.1.1.1 For the following categories of records, a system shall be implemented to uniquely identify each record. This may include using codes, numbers, or other identifiers that make it easy to track, retrieve, and document specific records.

i. Application Records: Details of applicant information and prerequisites.
ii. Assessment Records: Examination results, interviews, practical evaluations.
iii. Certification Records: Issued certificates, validity periods, and certification scope.
iv. Recertification Records: Renewal applications and compliance check records.
v. Appeals and Complaints Records: Complaints against certification decisions and appeals.
vi. Surveillance Records: Periodic monitoring reports of certified persons.
vii. Audit Records: Internal and external audit reports and findings.
viii. Policies ICTA/SD/Pol/YY
- where ICTA is the CB
- SD is Department
- Pol is document type
- YY is the document number

5.1.3 Classification & Indexing

5.1.3.1 Records shall be classified based on their function and indexed in the Records Management System (RMS). The classification criteria shall include:

i. Record Type (Application, Assessment, Certification, etc.)
ii. Date of Creation
iii. Owner/Responsible Person
iv. Retention Period
v. Confidentiality Level (Restricted, Internal, Public)

5.1.4 Metadata and Tagging

5.1.4.1 Each record shall have metadata fields such as:

i. Title (Descriptive Name of the Record)
ii. Creation Date
iii. Reference Number
iv. Associated Documents (e.g., related assessment or complaints)
v. Status (Active, Archived, Disposed)

5.1.5 Record Logging and Control

5.1.5.1 All records shall be logged in a Records Register (digital or manual). The register shall track:

i. Record Identifier
ii. Creation Date
iii. Responsible Department
iv. Current Status
v. Any Modifications or Annotations

5.1.6 Record Accessibility & Security

i. Access to records shall be role-based and controlled.
ii. Sensitive records (e.g., personal data, assessment results) shall be encrypted or stored in secured physical/digital locations.
iii. An audit log shall track all accesses and modifications.

5.1.7 Periodic Review and Validation

i. Regular reviews shall be conducted to ensure accuracy and compliance with ISO/IEC 17024.
ii. Any misclassified records shall be corrected and documented.
iii. Duplicate records shall be merged, and obsolete records flagged for disposal as per the retention policy.

5.1.8 Internal audits shall verify the accuracy, consistency, and security of the records identification process. Any non-conformities shall be addressed through corrective actions.

5.2 Classification of Records for (view storage How hard copies are stored in file, lockable cabinets etc and soft copies in the server etc)

5.2.1 Records shall be stored in either physical format (paper) or electronic format (digital) and classified accordingly:

i. Active Records: Frequently accessed records stored in easily accessible locations.
ii. Archived Records: Infrequently accessed records stored securely for retention purposes.
iii. Confidential Records: Sensitive records stored with restricted access based on security classification.

5.2 Classification of Records for Storage

5.2.1 General

5.2.1.1 Records shall be stored in either physical (paper) or electronic (digital) format.

5.2.1.2 All records shall be classified based on their usage frequency and sensitivity level, as follows:

i. Active Records: Frequently accessed records stored in easily accessible but secure locations.
ii. Archived Records: Infrequently accessed records retained for legal, historical, or reference purposes.
iii. Confidential Records: Sensitive records requiring restricted access and additional security controls.

5.2.2 Physical Records Storage

5.2.2.1 Secure Storage Areas:

i. Physical records shall be stored in lockable cabinets, fireproof safes, or secure file rooms to protect against unauthorized access, fire, and water damage.
ii. Access to these cabinets or rooms shall be limited to authorized personnel only, using keys, access cards, or other security mechanisms.

5.2.2.2. Restricted Access:

i. A register of authorized personnel shall be maintained and regularly updated. This register shall include the individual's name, department, and level of access.
ii. Individuals not on the register must obtain written approval or be accompanied by authorized personnel before accessing any physical records.

5.2.2.3 Environmental Controls:

i. Storage areas shall be maintained at appropriate temperature and humidity levels to prevent deterioration of records.
ii. Regular inspections shall be conducted to ensure the integrity and legibility of stored documents.

5.2.2.4 Retention and Disposal:

i. Physical records shall be retained in accordance with the Record Retention Schedule.
ii. Upon reaching the end of their retention period or becoming obsolete, records shall be securely shredded or otherwise destroyed, with destruction logged in the Document Destruction Log.

5.2.2.5 Electronic Records Storage

i. Electronic records shall be stored on secure servers within the ICTA intranet or an approved cloud environment.
ii. Role-based access controls (RBAC) shall be used to ensure only authorized personnel can view, edit, or delete records.

5.2.2.5.2 Data Integrity and Confidentiality:

i. Files shall be saved in secure, non-editable formats (e.g., PDF/A) when necessary to preserve content integrity.

ii. Confidential records (e.g., personal data, financial documents) shall be encrypted both at rest and in transit.

5.2.2.5.3 Version Control and Backups:

i. Version control software or functionality shall be used to track changes and ensure the most current version is easily identifiable.

ii. Automated backups shall be performed on a regular schedule and stored off-site or in a secure cloud repository to facilitate disaster recovery.

5.2.2.5.4 Access Monitoring:

i. All electronic access attempts and modifications shall be logged to maintain an audit trail.

ii. Regular reviews of access logs shall be conducted to detect and address any unauthorized activities.

5.2.2.5.5 Retention and Archiving:

i. Electronic records shall be retained in accordance with the Record Retention Schedule, mirroring the same timelines and disposal criteria as physical records.

ii. Archived records shall be clearly marked as "Archived" or "Obsolete" (as applicable) and moved to a designated secure folder or server location with read-only access.

5.2.2.6 Review and Maintenance of Records

i. The Quality Manager (or designated personnel) shall periodically review both physical and electronic records to ensure continued relevance, accuracy, and security.

ii. Any records determined to be obsolete, incorrect, or no longer required shall be handled per the disposal guidelines in Section X.X (Document Destruction Log and Obsolete Document Log).

5.2.2.7 Confidentiality and Security

i. All personnel handling sensitive or confidential records shall sign a Confidentiality Agreement, ensuring compliance with data protection regulations and internal policies.

ii. Any breach or suspected breach of confidentiality shall be reported immediately to the Quality Manager for investigation and corrective action.

5.2.2.8 Physical Records Storage

5.2.2.8.1 Physical records shall be stored in fireproof, waterproof, and locked filing cabinets within a secure records room.

5.2.2.8.2 Access to the records room shall be restricted to authorized personnel only.

5.2.2.8.3 A register of personnel authorized to access physical records shall be maintained.

5.2.2.9 Organization & Labelling

5.2.2.9.1 Documents shall be stored chronologically and grouped by record type.

5.2.2.9.2 Each document shall be assigned a unique identifier for tracking purposes.

5.2.2.10 Backup & Redundancy

5.2.2.2.1 Critical physical records shall be scanned and backed up digitally to mitigate risks of damage or loss.

5.2.3 Electronic Records Storage

5.2.3.1 Storage Systems Electronic records shall be stored using the Authority Intranet.

5.2.3.2.1 Metadata shall be assigned to each record, including:

i. Title (Descriptive document name)
ii. Date Created
iii. Responsible Department
iv. Retention Period

5.2.3.3 Access Control & Security

5.2.3.3.1 Role-Based Access Control (RBAC) shall be enforced to restrict access to authorized personnel only.

5.2.3.3.2 Audit logs shall track all access and modifications.

5.2.3.4 Regular Backups

5.2.3.5 Automated backups shall occur every 24 hours

5.3 Records Protection Procedures

5.3.1 Records shall be classified based on their sensitivity and level of protection required:

5.3.1.1 Confidential Records: High-risk records requiring restricted access (e.g., certification decisions, assessment results).

5.3.1.2 Internal Records: Operational records accessible to authorized internal personnel only.

5.3.1.3 Public Records: Non-sensitive records that may be publicly available (e.g., certification scope details).

5.3.2 Secure Storage Locations

5.3.2.1 All physical records shall be stored in fireproof, waterproof, and lockable cabinets in a secure records room.

5.3.2.2 Access to the records room shall be restricted to authorized personnel only.

5.3.2.3 Surveillance systems (CCTV) shall monitor access to storage areas.

5.3.3 Access Control

5.3.3.1 Access logbooks shall be maintained to track who accessed physical records and when.

5.3.3.2 Only pre-authorized personnel shall have access to confidential physical records.

5.3.4 Fire and Disaster Protection

5.3.4.1 Fire suppression systems (e.g., smoke detectors, fire extinguishers) shall be installed in all record storage areas.

5.3.5 Electronic Records Protection

5.3.5.1 Electronic records shall be stored in the Records Management System (RMS)

5.3.5.2 Files shall be protected with password authentication for critical documents.

5.3.5.3 Role-based access Control (RBAC) shall be enforced, limiting access based on job roles and security levels.

5.3.5.4 Audit logs shall track every access, modification, or deletion of records.

5.3.5.5 Automated daily backups shall be performed, with weekly off-site storage for redundancy.

5.3.5.6 A read-only mode shall be enabled for final records to prevent unauthorized modifications.

5.4 Retrieval Procedures

5.4.1 Records shall be retrieved stored chronologically for ease of retrieval on their classification and access level:

i. Public Records: Freely accessible upon request

ii. Internal Use Records: Available to authorized personnel within ICT Authority.

iii. Confidential Records: Restricted access requiring authorization before retrieval.

5.4.2 Each record type shall be retrieved according to its security classification to prevent unauthorized access.

5.4.3 Physical Records Retrieval

5.4.3.1 Employees requesting physical records must submit a Records Retrieval Request Form to the Records Officer.

5.4.3.2 Confidential records require additional approval from the Certification Manager.

5.4.3.3 The Records Officer retrieves the requested file from the secure storage area.

5.4.3.4 An access logbook must be maintained, capturing:

i. Name of requester

ii. Record details

iii. Date and time of retrieval

iv. Purpose of access

5.4.3.5 The requester shall acknowledge receipt of the record by signing the logbook.

5.4.3.6 Temporary Access & Return

5.4.3.6.1 Retrieved records must be returned within the stipulated timeframe

5.4.3.6.2 The Records Officer verifies and logs the return of the document in the Records Register.

5.4.4 Electronic Records Retrieval

5.4.4.1 Retrieval through the Records Management System (RMS)Digital records shall be accessed via the Records Management System (RMS) using role-based authentication.

5.4.4.2 Requests for confidential records require formal approval from the Certification Manager.

5.4.4.3 Approved records shall be shared via secured digital channels (e.g., encrypted email, restricted-access cloud folder).

5.4.4.4 Read-only access shall be granted where necessary to prevent modifications.

5.4.4.5 Audits shall be conducted to verify proper retrieval procedures.

5.4.4.6 Any unauthorized access attempts shall be investigated immediately.

5.4.4.7 The Records Officer shall maintain an audit log for accountability.

5.5 Retention

5.5.1 The ICT Authority shall manage records by ensuring:

i. Records are retained in accordance with legal, regulatory, and ISO/IEC 17024 requirements.
ii. records are protected from unauthorized access and loss.
iii. Certification decisions remain verifiable through record retention policies.

5.5.2 Records shall be classified based on their function and required retention period:

i. Permanent Retention: Records with legal, regulatory, or historical importance (e.g., certification decisions, appeals).
ii. Long-Term Retention (5-10 years): Records necessary for compliance and reference (e.g., assessment records, surveillance reports).
iii. Medium-Term Retention (3-5 years): Operational records required for monitoring certification status (e.g., complaints, recertification).
iv. Short-Term Retention (1-3 years): Temporary records not critical for future reference (e.g., general correspondence, administrative logs).

5.5.3 Each record type shall have an assigned retention period to ensure compliance with legal and accreditation requirements.

5.5.4 Retention Periods: The following retention periods shall apply:

Record Type	Retention Period
Certification Decisions & Appeals	Permanent
Assessment & Exam Records	10 years
Complaints & Disciplinary Actions	5 years
Recertification Records	5 years
Audit Reports & Surveillance Data	5 years
General Correspondence & Logs	3 years

5.5.5 Retention periods shall be reviewed annually to ensure compliance with legal and accreditation requirements.

5.5.6 Physical Records Retention

5.5.7 Electronic Records Retention

5.5.7.1 Digital records shall be stored in the intranet and access controls.

5.5.7.2 Retention periods shall be automated, ensuring timely archival and disposal of expired records

5.5.7.3 Records with long-term retention shall be archived in read-only mode to prevent unauthorized modifications.

5.5.7.4 Audit logs shall track record modifications and access.

5.5.8 Disposal of Records

5.5.8.1 Records identified for disposal shall be categorized based on:

5.5.8.1.1.1 Confidential Records: Require secure destruction

5.5.8.1.1.2 General Operational Records: May be disposed of through standard waste management after approval.

5.5.8.1.1.3 Electronic Records: Require permanent deletion and removal from backup storage.

5.5.8.2 Each record type shall be assessed before disposal to prevent unauthorized destruction of required records.

5.5.8.3 Disposal Approval Process

5.5.8.4 The Records Officer shall generate a Records Disposal List detailing:

i. Record type
ii. Retention period
iii. Disposal method
iv. Approval authority

5.5.8.5 The Certification Manager shall review and approve the disposal of confidential records.

5.5.8.6 Disposal shall be documented in a Disposal Register, capturing

i. Date of disposal
ii. Reason for disposal
iii. Method used
iv. Personnel involved

5.5.8.6.1 Disposal of Physical Records Confidential records shall be shredded using cross-cut shredders or incinerated.

5.5.8.7 Shredding shall be conducted under supervision in a designated secure area.
5.5.8.7.1 Disposal of Electronic Records
5.5.8.7.2 Digital records shall be permanently erased using data-wiping software that meets industry standards
5.5.8.7.3 Backup copies shall be removed to prevent retrieval.
5.5.8.7.4 Hard drives, SSDs, and removable storage devices containing sensitive records shall be physically destroyed (e.g., degaussing, crushing).
5.5.8.7.5 A record of destruction shall be logged.
5.5.8.7.6 The Records Officer shall conduct a final verification before records are destroyed.
5.5.8.7.7 The Disposal Register shall be reviewed and signed off by the Certification Manager.
5.5.8.7.8 A quarterly audit shall be performed to ensure compliance with the ISO/IEC 17024 disposal policy.

5.5.9 Handwritten records

5.5.9.1 All handwritten records must be clearly legible, properly dated, and signed by the responsible authority before being considered official.
5.5.9.2 The certification body shall ensure that all handwritten documents are authorized, verified, and where necessary, digitized for consistency and accessibility.
5.5.9.3 Handwritten documents containing sensitive or confidential information must be securely stored and access restricted to authorized personnel only.
5.5.9.4 Confidentiality agreements shall be in place, and no document shall be disclosed without proper authorization unless required by law.
5.5.9.5 The use of handwritten records shall be strictly regulated, ensuring their integrity, traceability, and compliance with certification requirements.
5.5.9.6 All handwritten records must be retained for a defined period as per regulatory, contractual, and accreditation requirements.
5.5.9.7 Periodic reviews shall be conducted to ensure document accuracy, and where applicable, records should be transcribed into digital formats to enhance accessibility and long-term preservation.
5.5.9.8 Handwritten documents shall be securely archived or disposed of in accordance with documented procedures.
5.5.9.9 Sensitive records must be shredded or incinerated to prevent unauthorized access, while essential records shall be preserved in an appropriate storage system for future reference and audits."

6.0 COMMUNICATION AND TRAINING

6.1 All personnel handling records shall receive mandatory training on this procedure.
6.2 Periodic awareness sessions shall reinforce compliance.

7.0 INTERNAL DISSEMINATION

7.1 Updates shall be communicated via ICT Authority's intranet.
7.2 The latest version of this procedure shall be accessible on the certification portal.

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