RECORDS MANAGEMENT AND DATA SECURITY

1. Purpose

- The purpose of this policy is to establish a framework for the creation, management, protection, access, retention, and disposal of records and data handled by IQMCINDIA Certification Pvt. Ltd., in compliance with ISO/IEC 17021-1:2015 clause 9.9.
- It supports IQMCINDIA's commitment to:
- Ensuring the confidentiality, integrity, and availability of client and operational information.
- Protecting information against loss, misuse, unauthorized access, alteration, or destruction.
- Promoting transparency and traceability in certification-related records.

2. Scope

This policy applies to:

- All physical and electronic records related to certification and management system operations.
- All IQMCINDIA employees, auditors, and contracted personnel who handle records and data.
- All certification clients and their related information.

3. Definitions

- **Records**: Information created, received, and maintained as evidence of activities or decisions.
- **Confidential Data**: Any non-public data obtained from clients or internal sources, including audit findings and client documentation.
- **Information Security**: Protection of data from unauthorized access or modifications, ensuring confidentiality, integrity, and availability.
- **Access Control**: Restriction of data availability only to authorized individuals.
- **Backup**: Regular copying and secure storage of digital data to protect against loss or damage.

4. Records Management Principles

IQMCINDIA shall:

- Maintain accurate, complete, and up-to-date records to demonstrate compliance with certification procedures and decisions.
- Use standardized formats and templates for recordkeeping.
- Classify records (e.g., public, internal, confidential) and store them accordingly.
- Ensure records are retrievable, traceable, and available for internal/external audits and reviews.
- Implement version control to track changes and updates to key documents.

5. Retention and Disposal

- Records are retained in accordance with the Retention of Records Policy (IQMC-PY13).
- Disposal of records after their retention period must be:
- Documented

- Approved by authorized personnel
- Conducted securely (shredding for physical, permanent deletion for digital)

6. Data Security Controls

- IQMCINDIA implements the following controls to ensure data security:
- User authentication and password-protected access to digital systems
- Use of firewalls, antivirus software, and encrypted storage
- Role-based access control to limit data visibility
- Daily or weekly data backups with offsite or cloud redundancy
- Use of locked cabinets or access-controlled rooms for physical documents

7. Confidentiality and Staff Responsibilities

- All staff and contractors must sign a confidentiality agreement before accessing client records.
- Information is only shared with third parties with:
- Written client consent
- Legal or accreditation requirements
- Internal training ensures all employees understand:
- Confidential data handling
- Reporting data breaches or unauthorized access

8. Data Breach and Incident Response

- In the event of a data breach or unauthorized access:
- The Management Representative will investigate and document the incident.
- Affected clients or authorities will be informed (as per legal/accreditation rules).
- Corrective actions will be initiated to prevent recurrence.

9. Responsibilities

- Top Management ensures this policy is implemented, reviewed, and enforced.
- The Managing Director oversees:
- Record classification and storage
- Data access controls and security updates
- Digital backup systems
- Antivirus and encryption protocols
- All Employees must:
- Follow defined procedures
- Report any breaches or irregularities immediately

10. Review and Revision

- This policy shall be:
- Reviewed annually or when significant changes occur in regulations, or ISO standard revisions.
- Revised as needed to address identified risks, vulnerabilities, or improvements.

11. References

ISO/IEC 17021-1:2015 – Clauses- 4.6 and 8.4.7
IQMCINDIA Retention of Records Policy- IQMC-PY13
IQMCINDIA Confidentiality Policy- IQMC-PY04

Document Number: IQMC-PY09
Effective Date: 01.04.2023
Revision: REV05
Approval: Managing Director

IQMCINDIA CERTIFICATION PVT LTD

FOR MORE INFORMATION DO VISIT-: www.iqmcindia.com

Email -: iqmc.india@gmail.com or info@iqmcindia.com

Contact-: 0121-4050009 or +91-121-4050009