LIBERIA MEDICINES & HEALTH PRODUCTS REGULATORY AUTHORITY

[LMHRA]

Data Classification & Handling Policy

P.O BOX 1994
Cell: +231-777140555/888140555
Email: info@lmhra.gov.lr
Website: www.lmhra.gov.lr

Document Code: ICT-POL-001	**Date of Issue: April 13, 2026**
Version: 01	**Date of Implementation: April 16, 2026**

CONTENTS

1.0 PURPOSE....3
2.0 SCOPE....3
3.0 POLICY STATEMENT....4
4.0 GUIDING PRINCIPLES....4
5.0 DEFINITIONS....4
6.0 DATA CLASSIFICATION LEVELS....4
6.1 LEVEL 1 — PUBLIC....5
6.2 LEVEL 2 — INTERNAL....5
6.3 LEVEL 3 — CONFIDENTIAL....5
6.4 LEVEL 4 — HIGHLY CONFIDENTIAL (REGULATORY SENSITIVE)....6
7.0 DATA HANDLING REQUIREMENTS....6
7.1 DATA STORAGE....6
7.2 DATA TRANSMISSION....7
7.3 DATA ACCESS....7
7.4 DATA SHARING....7
7.5 DATA RETENTION....7
7.6 DATA DISPOSAL....7
8.0 ROLES AND RESPONSIBILITIES....7
9.0 MONITORING AND COMPLIANCE....8
10.0 VIOLATIONS AND ENFORCEMENT....8
11.0 POLICY REVIEW....9
12.0 APPROVAL....9

1.0 PURPOSE

The purpose of this Data Classification & Handling Policy is to ensure that all information processed, stored, transmitted, or managed by the Liberia Medicines and Health Products Regulatory Authority (LMHRA) is protected according to its sensitivity, regulatory importance, and legal requirements.

This policy establishes a standardized framework for classifying, labeling, storing, transmitting, and disposing of LMHRA data to safeguard confidentiality, integrity, and availability.

2.0 SCOPE

This policy applies to:

- All LMHRA staff, contractors, consultants, interns, and partners
- All LMHRA information assets (digital and physical)
- All ICT systems, applications, databases, and cloud services
- All devices accessing LMHRA data
- All third-party service providers handling LMHRA information

3.0 POLICY STATEMENT

LMHRA is committed to protecting its information assets through a structured data classification and handling framework. All LMHRA data must be classified according to sensitivity and handled in accordance with this policy to prevent unauthorized access, misuse, disclosure, alteration, or loss.

4.0 GUIDING PRINCIPLES

- **Confidentiality** — Sensitive data must be protected from unauthorized access.
- **Integrity** — Data must remain accurate, complete, and unaltered.
- **Availability** — Data must be accessible to authorized users when needed.
- **Compliance** — Align with ISO 27001, ISO 27002, WHO guidelines, and national regulations.
- **Least Privilege** — Access to data is granted strictly based on job requirements.
- **Accountability** — All users are responsible for protecting LMHRA data.

5.0 DEFINITIONS

- **Data Owner:** Department responsible for the data and its classification.

- **Data Custodian:** ICT Unit responsible for implementing controls.
- **Data User:** Any individual accessing LMHRA data.
- **Sensitive Data:** Information requiring protection due to regulatory, legal, or operational impact.
- **Highly Confidential Data:** Data whose unauthorized disclosure could cause severe harm to public health, regulatory integrity, or LMHRA operations.

6.0 DATA CLASSIFICATION LEVELS

LMHRA classifies data into four levels:

6.1 LEVEL 1 — PUBLIC

Description:

Information approved for public release.

Examples:

- Public advisories
- Press releases
- Approved public reports
- Website content

Handling Requirements:

- No special restrictions
- Must be verified for accuracy before publication

6.2 LEVEL 2 — INTERNAL

Description:

Information intended for internal LMHRA use only.

Examples:

- Internal memos
- Routine administrative documents
- Non-sensitive operational data

Handling Requirements:

- Access limited to LMHRA staff
- Must not be shared externally without authorization
- Stored on LMHRA-approved systems

6.3 LEVEL 3 — CONFIDENTIAL

Description:

Sensitive information that could cause harm if disclosed.

Examples:

- Staff records
- Procurement documents
- Inspection reports
- Non-public regulatory data
- System configuration files

Handling Requirements:

- Access restricted to authorized personnel
- Encryption required for storage and transmission
- Must not be emailed externally without approval
- Printed copies must be secured

6.4 LEVEL 4 — HIGHLY CONFIDENTIAL (REGULATORY SENSITIVE)

Description:

Critical regulatory information whose unauthorized disclosure could severely impact public health, national security, or LMHRA operations.

Examples:

- Product registration dossiers
- Pharmacovigilance case reports
- Quality control laboratory results
- Enforcement and investigation data
- GMP related documents
- Clinical Trial Protocols
- Security credentials and encryption keys etc.

Handling Requirements:

- Strict need-to-know access
- Mandatory encryption at rest and in transit
- Prohibited from being stored on personal devices
- Must not be transmitted via unsecured channels
- Physical copies must be locked in secure cabinets

- Disposal must follow secure destruction procedures

7.0 DATA HANDLING REQUIREMENTS

7.1 DATA STORAGE

- All LMHRA data must be stored on LMHRA-approved servers, cloud platforms, or devices.
- Highly Confidential data must be encrypted using approved encryption standards.
- Portable storage devices require ICT approval and encryption.

7.2 DATA TRANSMISSION

- Confidential and Highly Confidential data must be encrypted during transmission.
- Emailing sensitive data externally requires authorization from the Data Owner.
- Public Wi-Fi must not be used for accessing LMHRA systems unless via secure VPN.

7.3 DATA ACCESS

- Access must follow the Access Control Policy.
- Data Owners determine access rights.
- Access must be reviewed quarterly.

7.4 DATA SHARING

- Sharing with external parties requires:
    - A signed confidentiality agreement
    - Approval from the Data Owner
    - Verification of recipient identity
- Highly Confidential data may only be shared through secure channels.

7.5 DATA RETENTION

- Data must be retained according to LMHRA's Records Management Policy.
- Retention periods must comply with regulatory and legal requirements.

7.6 DATA DISPOSAL

- Public and Internal data may be disposed of using standard methods.
- Confidential and Highly Confidential data must be destroyed securely:
    - Shredding (physical documents)
    - Secure wipe or cryptographic erasure (digital data)
- Disposal must be documented and verified.

8.0 ROLES AND RESPONSIBILITIES

Managing Director

- Provides oversight and approves the policy.

ICT Manager (Policy Owner)

- Implements and enforces data classification controls.
- Ensures secure storage, transmission, and disposal mechanisms.

Data Owners (Department Heads)

- Classify data under their control.
- Approve access and sharing requests.
- Ensure compliance within their departments.

Data Custodians (ICT Unit)

- Apply technical controls (encryption, access control, backups).
- Monitor data handling activities.

All Staff

- Handle data according to classification requirements.
- Report any suspected data breaches immediately.

Vendors & Third Parties

- Must comply with LMHRA data protection requirements.
- Must notify LMHRA of any breach affecting LMHRA data.

9.0 MONITORING AND COMPLIANCE

- ICT Unit must monitor access logs and data movement.

- Internal audits must be conducted annually.
- Violations must be reported to Executive Management.

10.0 VIOLATIONS AND ENFORCEMENT

Non-compliance may result in:

- Disciplinary action
- Revocation of access privileges
- Contract termination (for vendors)
- Legal action where applicable

11.0 POLICY REVIEW

This policy must be reviewed:

- After three years
- After major incidents
- After significant organizational or technological changes

The ICT Manager is responsible for initiating the review.

12.0 APPROVAL

This policy becomes effective upon approval by the Managing Director of LMHRA.

The Data Classification & Handling Policy is Hereby Promulgated and Approved by the Managing Director on this 13th Day of April A. D. 2026.



Hon. Luke L Bawo
Managing Director / LMHRA