LIBERIA MEDICINES & HEALTH PRODUCTS REGULATORY AUTHORITY

[LMHRA]

Information Security Policy

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

Document Code: ICT-POL-003	**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 3
4.0 GUIDING PRINCIPLES 3
5.0 DEFINITIONS 3
6.0 INFORMATION SECURITY OBJECTIVES 4
7.0 INFORMATION SECURITY GOVERNANCE 4
7.1 GOVERNANCE STRUCTURE 4
8.0 ACCESS CONTROL POLICY 4
9.0 ACCEPTABLE USE POLICY 5
10.0 NETWORK & INFRASTRUCTURE SECURITY 5
11.0 DATA SECURITY & CLASSIFICATION 5
12.0 PHYSICAL SECURITY 5
13.0 APPLICATION & SYSTEM SECURITY 5
14.0 CLOUD & THIRD-PARTY SECURITY 6
15.0 BACKUP & RECOVERY 6
16.0 INCIDENT MANAGEMENT 6
17.0 BUSINESS CONTINUITY & DISASTER RECOVERY 6
18.0 SECURITY AWARENESS & TRAINING 6
19.0 MONITORING & AUDIT 7
20.0 POLICY COMPLIANCE 7
21.0 POLICY REVIEW 7
22.0 APPROVAL 7

1.0 PURPOSE

The purpose of this Information Security Policy is to protect the confidentiality, integrity, and availability of all information assets managed by the Liberia Medicines and Health Products Regulatory Authority (LMHRA).

The policy establishes mandatory requirements for safeguarding regulatory data, ICT systems, infrastructure, and digital services against unauthorized access, misuse, disclosure, disruption, modification, or destruction.

2.0 SCOPE

This policy applies to:

- All LMHRA staff, contractors, consultants, interns, and partners
- All LMHRA information assets, including electronic and paper records
- All ICT systems, networks, applications, and cloud services
- All devices accessing LMHRA data (LMHRA-owned or BYOD where permitted)
- All third-party service providers with access to LMHRA systems

3.0 POLICY STATEMENT

LMHRA is committed to maintaining a secure information environment that supports its regulatory mandate. All users must comply with this policy to ensure that information is protected from internal and external threats, and that LMHRA meets national and international standards for information security.

4.0 GUIDING PRINCIPLES

- **Confidentiality** — Information is accessible only to authorized individuals.
- **Integrity** — Information is accurate, complete, and protected from unauthorized modification.
- **Availability** — Information and systems are accessible when required.
- **Accountability** — All users are responsible for protecting LMHRA information assets.
- **Compliance** — Align with ISO 27001and national ICT regulations.
- **Least Privilege** — Access is granted strictly based on job requirements.
- **Continuous Improvement** — Security controls evolve with emerging threats.

5.0 DEFINITIONS

- **Information Asset:** Any data, system, device, or resource that supports LMHRA operations.
- **User:** Any individual accessing LMHRA information or systems.

- **Information Security Incident:** Any event that compromises confidentiality, integrity, or availability.
- **Access Control:** Mechanisms that restrict access to authorized users.
- **Malware:** Malicious software designed to disrupt or damage systems.

6.0 INFORMATION SECURITY OBJECTIVES

1. Protect regulatory data from unauthorized access or disclosure.
2. Ensure continuity of LMHRA operations.
3. Reduce exposure to cybersecurity threats.
4. Strengthen compliance with national and international standards.
5. Promote a culture of security awareness across LMHRA.

7.0 INFORMATION SECURITY GOVERNANCE

7.1 GOVERNANCE STRUCTURE

- **Managing Director** — Provides strategic oversight and approves the policy.
- **ICT Manager** — Policy owner; responsible for implementation and monitoring.
- **ICT Unit** — Implements technical and administrative controls.
- **Department Heads** — Ensure compliance within their departments.
- **All Staff** — Must follow security procedures and report incidents.
- **Vendors/Contractors** — Must comply with LMHRA security requirements.

8.0 ACCESS CONTROL POLICY

- Access to systems and data must be based on **role-based access control (RBAC).**
- User accounts must be unique and not shared.
- Strong passwords and multi-factor authentication (MFA) must be used where available.
- Access rights must be reviewed quarterly.
- Accounts must be disabled immediately upon staff separation.

9.0 ACCEPTABLE USE POLICY

Users must:

- Use LMHRA ICT resources only for authorized purposes.
- Protect passwords and never share them.
- Avoid accessing inappropriate or malicious websites.
- Not installing unauthorized software.
- Not connect unauthorized devices to LMHRA networks.

10.0 NETWORK & INFRASTRUCTURE SECURITY

- Firewalls, intrusion detection/prevention systems, and endpoint protection must be implemented.
- Network segmentation must be used to isolate critical systems.
- Wireless networks must use secure authentication and encryption.
- Remote access must be secured using VPN and MFA.
- Regular vulnerability scans must be conducted.

11.0 DATA SECURITY & CLASSIFICATION

LMHRA data must be classified into:

- **Public**
- **Internal**
- **Confidential**
- **Highly Confidential (Regulatory Sensitive)**

Controls must match classification levels.

Confidential and Highly Confidential data must be encrypted in transit and at rest.

12.0 PHYSICAL SECURITY

- Server rooms must be locked and accessible only to authorized personnel.
- Visitors must be escorted at all times.
- CCTV and access logs must be maintained.
- Devices must not be left unattended in public areas.

13.0 APPLICATION & SYSTEM SECURITY

- All systems must be patched regularly.
- Secure configuration baselines must be applied.

- Default passwords must be changed immediately.
- Application development must follow secure coding practices.
- Third-party applications must undergo security assessment.

14.0 CLOUD & THIRD-PARTY SECURITY

- Cloud providers must meet recognized security standards (ISO 27001).
- Data stored in the cloud must be encrypted.
- Third-party contracts must include security clauses.
- Vendors must notify LMHRA of any breaches affecting LMHRA data.

15.0 BACKUP & RECOVERY

- Critical data must be backed up daily.
- Backups must be stored securely offsite or in the cloud.
- Backup restoration must be tested quarterly.
- Backup access must be restricted.

16.0 INCIDENT MANAGEMENT

- All staff must report security incidents immediately to the ICT Unit.
- The ICT Unit must log, investigate, and resolve incidents.
- Major incidents must be escalated to Managing Management.
- Post-incident reviews must be conducted to prevent recurrence.

17.0 BUSINESS CONTINUITY & DISASTER RECOVERY

- LMHRA must maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
- Critical systems must have redundancy.
- Annual DRP testing is required.

18.0 SECURITY AWARENESS & TRAINING

- All staff must receive annual information security training.
- Specialized training must be provided for ICT staff.
- Awareness campaigns must be conducted regularly.

19.0 MONITORING & AUDIT

- ICT systems must be monitored for suspicious activity.
- Logs must be retained and reviewed regularly.
- Annual internal and external audits must be conducted.
- Non-compliance must be addressed promptly.

20.0 POLICY COMPLIANCE

Non-compliance may result in:

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

21.0 POLICY REVIEW

This policy must be reviewed:

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

The ICT Manager is responsible for initiating the review.

22.0 APPROVAL

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

The* Information Security 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