LIBERIA MEDICINES & HEALTH PRODUCTS REGULATORY AUTHORITY

[LMHRA]

ICT Policy

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

Document Code: ICT-POL-010	**Date of Issue: April 13, 2026**
Version: 01	**Date of Implementation: April 16, 2026**

CONTENTS

1.0 PURPOSE....4
2.0 SCOPE....4
3.0 GOVERNANCE AND LEADERSHIP....4
3.1 ICT GOVERNANCE STRUCTURE....4
3.2 POLICY REVIEW....4
4.0 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)....5
5.0 ASSET MANAGEMENT....5
5.1 ASSET INVENTORY....5
5.2 ASSET CLASSIFICATION....5
6.0 ACCESS CONTROL....5
6.1 USER ACCESS MANAGEMENT....5
6.2 AUTHENTICATION REQUIREMENTS....6
6.3 PRIVILEGED ACCESS....6
7.0 NETWORK AND INFRASTRUCTURE SECURITY....6
7.1 NETWORK SEGMENTATION....6
7.2 FIREWALLS AND FILTERING....6
7.3 PATCH AND VULNERABILITY MANAGEMENT....6
8.0 DATA PROTECTION AND PRIVACY....6
8.1 DATA HANDLING....6
8.2 DATA BACKUP....6
8.3 DATA RETENTION....7
9.0 ACCEPTABLE USE POLICY (AUP)....7
10. SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT....7
10.1 CHANGE CONTROL....7
10.2 SECURE DEVELOPMENT....7
11.0 INCIDENT MANAGEMENT....7
11.1 REPORTING....7
11.2 RESPONSE PROCESS....8

12.0 BUSINESS CONTINUITY AND DISASTER RECOVERY 8
13. SUPPLIER AND THIRD-PARTY MANAGEMENT 8
14.0 PHYSICAL AND ENVIRONMENTAL SECURITY 8
15.0 TRAINING AND AWARENESS 8
16.0 COMPLIANCE 9
17.0 CONTINUOUS IMPROVEMENT 9

1.0 PURPOSE

The purpose of this ICT Policy is to establish a secure, reliable, and efficient Information and Communication Technology (ICT) environment for the Liberia Medicines and Health Products Regulatory Authority (LMHRA). This policy ensures that all information assets—systems, data, infrastructure, and services—are protected in accordance with **ISO/IEC 27001:2022** standards for information security management.

2.0 SCOPE

This policy applies to:

- All LMHRA staff, contractors, consultants, interns, and temporary workers
- All LMHRA ICT systems, including MIS platforms, databases, networks, servers, cloud services, and communication tools
- All information processed, stored, transmitted, or accessed through LMHRA systems
- All LMHRA facilities where ICT assets are located

3.0 GOVERNANCE AND LEADERSHIP

3.1 ICT GOVERNANCE STRUCTURE

- The **Managing Director** provides executive oversight.
- The **ICT Unit** is responsible for implementing, monitoring, and maintaining ICT controls.
- The **ICT Manager** serves as the **Information Security Officer (ISO)** for ISO27001 alignment.
- Each department must designate an **Information Asset Owner**.

3.2 POLICY REVIEW

This policy shall be reviewed **annually** or after major system changes, security incidents, or regulatory updates.

4.0 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

LMHRA shall maintain an ISMS consistent with ISO/IEC 27001:2022, including:

- Risk assessment and treatment
- Asset management
- Access control
- Incident management
- Business continuity
- Supplier management
- Continuous improvement

5.0 ASSET MANAGEMENT

5.1 ASSET INVENTORY

The ICT Unit shall maintain an updated inventory of:

- Hardware
- Software
- Network devices
- Databases
- Cloud services
- User accounts
- Licenses

5.2 ASSET CLASSIFICATION

Information shall be classified as:

Classification	Description
Public	Approved for public release
Internal	For internal LMHRA use only
Confidential	Sensitive regulatory, operational, or personal data
Restricted	High-risk data requiring strict controls

6.0 ACCESS CONTROL

6.1 USER ACCESS MANAGEMENT

- Access is granted based on **least privilege** and **need-to-know** principles.
- All accounts must be uniquely identifiable.
- Shared accounts are prohibited except for approved service accounts.
- Access rights must be reviewed **quarterly**.

6.2 AUTHENTICATION REQUIREMENTS

- Strong passwords required (minimum length, complexity, expiration).
- Multi-factor authentication (MFA) must be used for:
    - MIS administrative accounts
    - Remote access
    - Cloud services

6.3 PRIVILEGED ACCESS

- Admin accounts must be separated from normal user accounts.
- All privileged activities must be logged and monitored.

7.0 NETWORK AND INFRASTRUCTURE SECURITY

7.1 NETWORK SEGMENTATION

LMHRA shall maintain segmented networks for:

- MIS and regulatory systems
- Administrative systems
- Guest Wi-Fi
- Servers and critical infrastructure

7.2 FIREWALLS AND FILTERING

- Firewalls must be configured to allow only necessary traffic.
- Web filtering must block malicious or inappropriate sites.

7.3 PATCH AND VULNERABILITY MANAGEMENT

- All systems must be patched monthly or sooner for critical vulnerabilities.
- Vulnerability scans must be conducted **quarterly**.

8.0 DATA PROTECTION AND PRIVACY

8.1 DATA HANDLING

- Confidential and restricted data must be encrypted at rest and in transit.
- Personal data must be processed in accordance with national data protection principles.

8.2 DATA BACKUP

- Daily incremental backups
- Weekly full backups
- Offsite or cloud backup storage

- Quarterly restoration testing

8.3 DATA RETENTION

Retention schedules must align with:

- LMHRA regulatory requirements
- National laws
- Donor or partner agreements

9.0 ACCEPTABLE USE POLICY (AUP)

All users must:

- Use LMHRA ICT resources for official purposes
- Avoid installing unauthorized software
- Not bypass security controls
- Not use LMHRA systems for political, abusive, or illegal activities
- Report suspicious activity immediately

10. SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

10.1 CHANGE CONTROL

All changes to MIS systems must follow a documented process:

- Request
- Impact assessment
- Approval
- Testing
- Deployment
- Documentation

10.2 SECURE DEVELOPMENT

- Security requirements must be included in all system upgrades or new systems.
- Third-party developers must comply with LMHRA security standards.

11.0 INCIDENT MANAGEMENT

11.1 REPORTING

All staff must report incidents such as:

- Malware infections
- Unauthorized access

- Data loss
- System outages
- Suspicious emails

11.2 RESPONSE PROCESS

The ICT Unit shall maintain an Incident Response Plan including:

- Identification
- Containment
- Eradication
- Recovery
- Post-incident review

12.0 BUSINESS CONTINUITY AND DISASTER RECOVERY

LMHRA shall maintain:

- A Business Continuity Plan (BCP)
- A Disaster Recovery Plan (DRP)
- Redundant power systems (UPS, generator)
- Offsite backups
- Annual simulation exercises

13. SUPPLIER AND THIRD-PARTY MANAGEMENT

- All vendors must sign confidentiality and data protection agreements.
- Third-party systems must undergo security assessment before integration.
- Cloud providers must meet international security standards.

14.0 PHYSICAL AND ENVIRONMENTAL SECURITY

- Server rooms must be access-controlled and monitored.
- Fire suppression systems must be installed.
- Equipment must be protected from power fluctuations.
- Visitors must be escorted.

15.0 TRAINING AND AWARENESS

- Mandatory annual cybersecurity training for all staff
- Specialized training for ICT personnel
- Phishing simulations

- Awareness posters and reminders

16.0 COMPLIANCE

LMHRA shall comply with:

- ISO/IEC 27001:2022
- National ICT and cybersecurity regulations
- Public procurement laws
- Donor and partner requirements

Non-compliance may result in disciplinary action.

17.0 CONTINUOUS IMPROVEMENT

The ICT Unit shall:

- Conduct annual internal audits
- Track corrective and preventive actions
- Update controls based on emerging threats
- Maintain documentation for ISO27001 certification readiness

The ICT Policy is Hereby Promulgated and Approved by the Managing Director on this 13th Day of February A. D. 2026.



Hon. Luke L Bawo
Managing Director / LMHRA