LIBERIA MEDICINES & HEALTH PRODUCTS REGULATORY AUTHORITY

[LMHRA]

Access Control Policy

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

Document Code: ICT-POL-006	**Date of Issue: February 13, 2026**
Version: 01	**Date of Implementation: February 16, 2026**

CONTENTS

1.0 PURPOSE....3
2.0 SCOPE....4
3.0 POLICY STATEMENT....4
4.0 GUIDING PRINCIPLES....4
5.0 DEFINITIONS....4
6.0 ACCESS CONTROL OBJECTIVES....5
7.0 USER ACCOUNT MANAGEMENT....5
7.1 ACCOUNT CREATION....5
7.2 PASSWORD REQUIREMENTS....5
7.3 MULTI-FACTOR AUTHENTICATION (MFA)....5
7.4 ACCOUNT REVIEW....6
7.5 ACCOUNT TERMINATION....6
8.0 PRIVILEGED ACCESS MANAGEMENT....6
9.0 ACCESS TO APPLICATIONS AND SYSTEMS....6
10.0 NETWORK ACCESS CONTROL....6
11.0 PHYSICAL ACCESS CONTROL....7
12.0 DATA ACCESS CONTROL....7
13.0 THIRD-PARTY AND VENDOR ACCESS....7
14.0 MONITORING AND LOGGING....7
15.0 VIOLATIONS AND ENFORCEMENT....8
16.0 POLICY REVIEW....8
17.0 APPROVAL....8

Access Control Policy

1.0 PURPOSE

The purpose of this Access Control Policy is to ensure that access to LMHRA information systems, applications, data, and physical ICT resources is granted only to authorized individuals based on business needs, job responsibilities, and security requirements.

This policy establishes the principles, rules, and procedures for managing user access in order to protect the confidentiality, integrity, and availability of LMHRA information assets.

2.0 SCOPE

This policy applies to:

- All LMHRA staff, contractors, consultants, interns, and partners
- All LMHRA 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
- All physical ICT facilities, including server rooms and network cabinets

3.0 POLICY STATEMENT

LMHRA is committed to enforcing strict access controls to ensure that only authorized individuals can access LMHRA systems and data. Access must be granted based on the principle of least privilege, regularly reviewed, and revoked promptly when no longer required.

4.0 GUIDING PRINCIPLES

- **Least Privilege** — Users receive only the minimum access required to perform their duties.
- **Need-to-Know** — Access to sensitive information is restricted to authorized personnel.
- **Role-Based Access Control (RBAC)** — Access is assigned based on job roles.
- **Accountability** — All access must be traceable to an individual user.
- **Separation of Duties** — Critical tasks must be divided to reduce risk.
- **Compliance** — Align with ISO 27001, ISO 27002, COBIT, ITIL, and national ICT regulations.

5.0 DEFINITIONS

- **User:** Any individual accessing LMHRA systems or data.
- **Access Rights:** Permissions granted to a user to perform specific tasks.

- **Privileged Account:** Accounts with elevated access (e.g., admin accounts).
- **Authentication:** Verification of a user's identity.
- **Authorization:** Granting access rights based on identity and role.
- **MFA (Multi-Factor Authentication):** Additional verification beyond passwords.

6.0 ACCESS CONTROL OBJECTIVES

1. Ensure only authorized users access LMHRA systems and data.
2. Protect sensitive regulatory information from unauthorized disclosure.
3. Prevent misuse of privileged accounts.
4. Ensure timely removal of access for separated or transferred staff.
5. Maintain auditability and accountability for all access activities.

7.0 USER ACCOUNT MANAGEMENT

7.1 ACCOUNT CREATION

- All user accounts must be approved by the relevant Department Head and the ICT Manager.
- Accounts must be created based on job roles and responsibilities.
- Shared or generic accounts are prohibited except for approved system accounts.

7.2 PASSWORD REQUIREMENTS

- Passwords must meet LMHRA's Password Policy standards.
- Passwords must not be shared or written down in insecure locations.
- Default passwords must be changed immediately upon first login.

7.3 MULTI-FACTOR AUTHENTICATION (MFA)

- MFA must be enabled for:
    - Email
    - Remote access
    - Cloud services
    - Administrative accounts

7.4 ACCOUNT REVIEW

- User access rights must be reviewed quarterly by the ICT Unit.
- Department Heads must validate access for their staff.

7.5 ACCOUNT TERMINATION

- Accounts must be disabled immediately when:
  - Employment ends
  - Contract ends
  - User transfers to another department
- ICT must receive HR notification within 24 hours of staff separation.

8.0 PRIVILEGED ACCESS MANAGEMENT

- Administrative privileges must be granted only to authorized ICT personnel.
- Privileged accounts must not be used for routine tasks.
- All privileged activities must be logged and monitored.
- Privileged passwords must be stored securely and changed regularly.
- Dual authorization must be used for high-risk administrative actions.

9.0 ACCESS TO APPLICATIONS AND SYSTEMS

- Access to applications (RIMS, EDMS, finance systems, etc.) must be role-based.
- System owners must approve access requests.
- Access to sensitive modules (e.g., product registration, inspections, PV data) must be restricted.
- System access logs must be retained and reviewed periodically.

10.0 NETWORK ACCESS CONTROL

- Only authorized devices may connect to LMHRA networks.
- Guest Wi-Fi must be isolated from internal networks.

- Network segmentation must be used to protect critical systems.
- Remote access must be secured using VPN and MFA.
- Unauthorized devices (USBs, personal laptops) are prohibited unless approved.

11.0 PHYSICAL ACCESS CONTROL

- Server rooms and network cabinets must be locked at all times.
- Access must be restricted to authorized ICT personnel.
- Visitors must be escorted and logged.
- Physical access logs must be reviewed monthly.

12.0 DATA ACCESS CONTROL

- Access to data must be based on classification levels:
    - Public
    - Internal
    - Confidential
    - Highly Confidential (Regulatory Sensitive)
- Confidential and Highly Confidential data must be encrypted.
- Data extraction or export must require approval from the data owner.

13.0 THIRD-PARTY AND VENDOR ACCESS

- Vendors must sign confidentiality and security agreements.
- Vendor access must be time-bound and monitored.
- Remote vendor access must be approved by the ICT Manager.
- Vendors must notify LMHRA of any security incidents affecting LMHRA data.

14.0 MONITORING AND LOGGING

- All access to critical systems must be logged.

- Logs must be protected from tampering.
- Logs must be reviewed regularly for suspicious activity.
- Anomalies must be investigated promptly.

15.0 VIOLATIONS AND ENFORCEMENT

Non-compliance with this policy may result in:

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

16.0 POLICY REVIEW

This policy must be reviewed:

- Annually
- After major ICT incidents
- After significant organizational or technological changes

The ICT Manager is responsible for initiating the review.

17.0 APPROVAL

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

The Access Control 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