LIBERIA MEDICINES & HEALTH PRODUCTS REGULATORY AUTHORITY

[LMHRA]

Backup and Data Recovery Policy

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

Document Code: ICT-POL-007	**Date of Issue: April 13, 2026**
Version: 01	**Date of Implementation: April 16, 2026**

CONTENTS

2.0 SCOPE 3
3.0 POLICY STATEMENT 3
4.0 GUIDING PRINCIPLES 3
5.0 DEFINITIONS 4
6.0 BACKUP OBJECTIVES 4
7.0 BACKUP REQUIREMENTS 4
7.1 DATA TO BE BACKED UP 4
7.2 BACKUP FREQUENCY 4
7.3 BACKUP STORAGE LOCATIONS 5
7.4 BACKUP RETENTION PERIODS 5
8.0 BACKUP SECURITY CONTROLS 5
9.0 DATA RECOVERY REQUIREMENTS 5
9.1 RECOVERY TIME OBJECTIVE (RTO) 5
9.2 RECOVERY POINT OBJECTIVE (RPO) 5
9.3 RECOVERY PROCEDURES 6
10.0 TESTING AND VALIDATION 6
11.0 ROLES AND RESPONSIBILITIES 6
12.0 INCIDENT MANAGEMENT 7
13.0 THIRD-PARTY AND CLOUD BACKUP REQUIREMENTS 7
14. BACKUP MEDIA DISPOSAL 7
15. MONITORING AND COMPLIANCE 7
16. VIOLATIONS AND ENFORCEMENT 7
17. POLICY REVIEW 8
18. APPROVAL 8

1.0 PURPOSE

The purpose of this Backup & Data Recovery Policy is to ensure that all critical LMHRA data, systems, and digital services are backed up regularly and can be restored promptly in the event of data loss, corruption, system failure, cyberattack, or disaster.
This policy establishes the standards, responsibilities, and procedures required to maintain data integrity, business continuity, and regulatory compliance.

2.0 SCOPE

This policy applies to:

- All LMHRA staff, contractors, consultants, and partners
- All LMHRA information systems, databases, applications, and servers
- All digital data stored, processed, or transmitted by LMHRA
- All cloud-based and on-premises storage environments
- All backup media and disaster recovery infrastructure

3.0 POLICY STATEMENT

LMHRA is committed to ensuring that critical data and systems are protected through reliable, secure, and tested backup and recovery processes. Backups must be performed regularly, stored securely, and tested periodically to ensure recoverability.

4.0 GUIDING PRINCIPLES

- **Availability** — Critical systems and data must be recoverable within acceptable timeframes.
- **Integrity** — Backups must be complete, accurate, and protected from corruption.
- **Confidentiality** — Backup data must be encrypted and protected from unauthorized access.
- **Resilience** — Backup and recovery processes must support business continuity.
- **Compliance** — Align with ISO 27001, ISO 27002, WHO guidelines, and national ICT regulations.

5.0 DEFINITIONS

- **Backup:** A copy of data stored to enable recovery in case of loss.
- **Recovery:** The process of restoring data or systems from backups.
- **RPO (Recovery Point Objective):** Maximum acceptable amount of data loss measured in time.
- **RTO (Recovery Time Objective):** Maximum acceptable downtime before service restoration.
- **Critical Systems:** Systems essential to LMHRA's regulatory operations.
- **Backup Media:** Storage used for backups (cloud, external drives, servers, tapes).

6.0 BACKUP OBJECTIVES

1. Ensure all critical LMHRA data is backed up regularly.
2. Protect backup data from unauthorized access, corruption, or loss.
3. Ensure timely restoration of systems and data after an incident.
4. Support LMHRA's Business Continuity and Disaster Recovery Plans.
5. Maintain compliance with regulatory and legal requirements.

7.0 BACKUP REQUIREMENTS

7.1 DATA TO BE BACKED UP

The following must be backed up:

- Regulatory databases (RIMS, PV, QC Lab systems)
- Email and communication systems
- File servers and shared drives
- Financial and HR systems
- System configurations and network settings
- Virtual machines and cloud-hosted services
- Critical documents and operational records

7.2 BACKUP FREQUENCY

- **Critical systems:** Daily incremental + weekly full backup
- **Non-critical systems:** Weekly full backup

- **Configuration files:** After every major change
- **Cloud systems:** As per vendor SLA + LMHRA internal schedule

7.3 BACKUP STORAGE LOCATIONS

Backups must be stored in:

- **Primary onsite backup repository**
- **Secondary offsite or cloud backup location**
- **Offline or immutable storage** for ransomware protection

At least one backup copy must always be stored offsite.

7.4 BACKUP RETENTION PERIODS

- Daily backups: retained for 14–30 days
- Weekly backups: retained for 3 months
- Monthly backups: retained for 1 year
- Annual backups: retained for 5–7 years (or per regulatory requirement)

Retention must comply with LMHRA's Records Management Policy.

8.0 BACKUP SECURITY CONTROLS

- All backup data must be encrypted at rest and in transit.
- Access to backup systems must be restricted to authorized ICT staff.
- Backup media must be stored in secure, access-controlled environments.
- Backup logs must be maintained and reviewed regularly.
- Backup systems must be protected with MFA and strong authentication.

9.0 DATA RECOVERY REQUIREMENTS

9.1 RECOVERY TIME OBJECTIVE (RTO)

- Critical systems: restore within **24 hours**
- Non-critical systems: restore within **72 hours**

9.2 RECOVERY POINT OBJECTIVE (RPO)

- Critical systems: maximum **24 hours** of data loss

- Non-critical systems: maximum **72 hours** of data loss

9.3 RECOVERY PROCEDURES

- ICT Unit must maintain documented recovery procedures.
- Recovery steps must be tested and updated regularly.
- Only authorized ICT personnel may perform recovery operations.

10.0 TESTING AND VALIDATION

- Backup restoration tests must be conducted **quarterly**.
- Full disaster recovery simulations must be conducted **annually**.
- Test results must be documented and reviewed by ICT Management.
- Failures must be corrected immediately and retested.

11.0 ROLES AND RESPONSIBILITIES

Executive Director

- Provides oversight and approves the policy.
- Ensures adequate resources for backup and recovery.

ICT Manager (Policy Owner)

- Oversees backup and recovery operations.
- Ensures compliance with this policy.
- Maintains backup infrastructure and documentation.
- Reports backup status to Executive Management.

ICT Unit Staff

- Perform backups and monitor backup jobs.
- Conduct recovery tests.
- Maintain backup logs and storage media.
- Secure backup systems and media.

Department Heads

- Identify critical data requiring backup.
- Ensure staff comply with data handling requirements.

All Staff

- Store data only on LMHRA-approved systems to ensure backups capture it.
- Report data loss incidents immediately.

12.0 INCIDENT MANAGEMENT

- Backup failures must be reported immediately to the ICT Manager.
- Data loss incidents must follow LMHRA's Incident Response Procedure.
- Critical incidents must be escalated to Executive Management.

13.0 THIRD-PARTY AND CLOUD BACKUP REQUIREMENTS

- Cloud providers must meet recognized security standards (ISO 27001, SOC 2).
- Backup SLAs must be included in vendor contracts.
- Third-party access to backup data must be strictly controlled.
- Vendors must notify LMHRA of any incidents affecting backup data.

14. BACKUP MEDIA DISPOSAL

- Backup media must be securely wiped or destroyed before disposal.
- Disposal must follow LMHRA's Data Classification & Handling Policy.
- Disposal activities must be documented and verified.

15. MONITORING AND COMPLIANCE

- ICT Unit must monitor backup success/failure daily.
- Logs must be retained for audit purposes.
- Annual internal audits must assess backup and recovery compliance.

16. VIOLATIONS AND ENFORCEMENT

Non-compliance may result in:

- Disciplinary action

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

17. POLICY REVIEW

This policy must be reviewed:

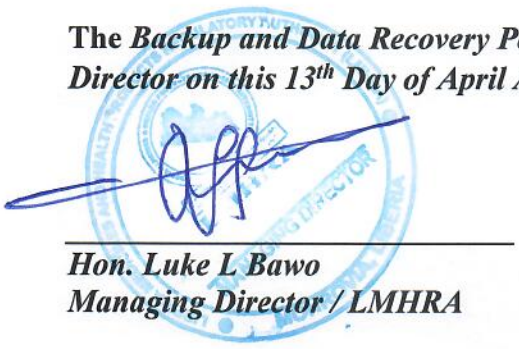
- After three years
- After major ICT incidents
- After significant technological or organizational changes

The ICT Manager is responsible for initiating the review.

18. APPROVAL

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

The *Backup and Data Recovery 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