LIBERIA MEDICINES & HEALTH PRODUCTS REGULATORY AUTHORITY

[LMHRA]

Disaster Recovery Policy

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

Document Code: ICT-POL-009	**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 POLICY STATEMENT....4
4.0 GUIDING PRINCIPLES....4
5.0 DEFINITIONS....5
6.0 DISASTER RECOVERY OBJECTIVES....5
7.0 DISASTER RECOVERY FRAMEWORK....5
7.1 DISASTER TYPES COVERED....5
7.2 ACTIVATION CRITERIA....6
8.0 CRITICAL SYSTEMS AND PRIORITIZATION....6
9.0 BACKUP REQUIREMENTS....6
10.0 DISASTER RECOVERY PROCEDURES....7
10.1 INITIAL RESPONSE....7
10.2 DAMAGE ASSESSMENT....7
10.3 RECOVERY ACTIONS....7
10.4 RETURN TO NORMAL OPERATIONS....7
11.0 ROLES AND RESPONSIBILITIES....8
12.0 COMMUNICATION DURING A DISASTER....8
13.0 TESTING AND MAINTENANCE....9
14.0 SECURITY AND COMPLIANCE....9
15.0 POLICY VIOLATIONS....9
16.0 POLICY REVIEW....9

Disaster Recovery Policy

17.0 APPROVAL.....10

1.0 PURPOSE

The purpose of this Disaster Recovery Policy is to ensure that LMHRA can restore critical ICT systems, data, and services in the event of a disaster, disruption, or major incident.
This policy establishes the framework, responsibilities, and procedures required to minimize downtime, protect regulatory data, and ensure continuity of LMHRA's public health mandate.

2.0 SCOPE

This policy applies to:

- All LMHRA ICT systems, applications, databases, and infrastructure
- All LMHRA staff, contractors, and third-party service providers
- All data stored, processed, or transmitted by LMHRA
- All cloud-based and on-premises environments
- All disaster scenarios affecting ICT operations (cyberattacks, fire, flood, power failure, hardware failure, etc.)

3.0 POLICY STATEMENT

LMHRA is committed to maintaining resilient ICT operations by implementing a structured Disaster Recovery (DR) framework that ensures rapid restoration of critical systems and data. DR procedures must be documented, tested, and continuously improved to support LMHRA's regulatory functions.

4.0 GUIDING PRINCIPLES

- **Resilience** — ICT systems must withstand and recover from disruptions.
- **Availability** — Critical services must be restored within acceptable timeframes.
- **Integrity** — Data must remain accurate and protected during recovery.
- **Preparedness** — DR plans must be maintained, tested, and updated.
- **Compliance** — Align with ISO 22301, ISO 27001, WHO guidelines, and national ICT regulations.
- **Accountability** — Roles and responsibilities must be clearly defined.

5.0 DEFINITIONS

- **Disaster:** Any event causing major disruption to ICT services.
- **Disaster Recovery (DR):** The process of restoring ICT systems and data after a disruption.
- **Business Continuity (BC):** Ensuring LMHRA operations continue during and after a disaster.
- **RTO (Recovery Time Objective):** Maximum acceptable downtime.
- **RPO (Recovery Point Objective):** Maximum acceptable data loss measured in time.
- **Critical Systems:** Systems essential to LMHRA's regulatory operations.

6.0 DISASTER RECOVERY OBJECTIVES

1. Restore critical ICT services within defined RTOs.
2. Minimize data loss through effective backup and recovery processes.
3. Ensure continuity of LMHRA's regulatory operations.
4. Protect LMHRA's reputation and public health mandate.
5. Maintain compliance with legal and regulatory requirements.

7.0 DISASTER RECOVERY FRAMEWORK

7.1 DISASTER TYPES COVERED

- Cyberattacks (ransomware, malware, DDoS)
- Hardware or system failure
- Power outages
- Fire, flood, or natural disasters
- Human error
- Network or telecommunications failure
- Cloud service outages

- Data corruption

7.2 ACTIVATION CRITERIA

The DR Plan must be activated when:

- Critical systems become unavailable
- Data integrity is compromised
- A disaster prevents normal ICT operations
- Executive Management or the ICT Manager declares a disaster

8.0 CRITICAL SYSTEMS AND PRIORITIZATION

LMHRA must maintain a list of critical systems, including:

- Regulatory Information Management System (RIMS)
- Pharmacovigilance (PV) systems
- Quality Control Laboratory systems
- Email and communication systems
- Financial and HR systems
- File servers and shared drives
- Network infrastructure and security systems

Each system must have defined:

- **RTO** (e.g., 24 hours for critical systems)
- **RPO** (e.g., 24 hours for critical data)

9.0 BACKUP REQUIREMENTS

Backups must follow LMHRA's Backup & Data Recovery Policy, including:

- Daily incremental and weekly full backups for critical systems
- Offsite or cloud storage for redundancy
- Encryption of all backup data
- Quarterly restoration testing
- Secure storage and access control

10.0 DISASTER RECOVERY PROCEDURES

The DR Plan must include detailed procedures for:

10.1 INITIAL RESPONSE

- Assess the incident
- Notify ICT Manager and Executive Management
- Activate the DR Team
- Contain the damage (e.g., isolate infected systems)

10.2 DAMAGE ASSESSMENT

- Identify affected systems
- Determine data loss or corruption
- Evaluate infrastructure damage

10.3 RECOVERY ACTIONS

- Restore systems from backups
- Rebuild servers or virtual machines
- Reconfigure network and security settings
- Validate system integrity
- Restore user access

10.4 RETURN TO NORMAL OPERATIONS

- Verify full system functionality
- Conduct post-recovery testing
- Document lessons learned
- Update DR procedures

11.0 ROLES AND RESPONSIBILITIES

Executive Director

- Approves DR Policy and major recovery decisions
- Ensures adequate resources for DR activities

ICT Manager (DR Lead)

- Activates and coordinates the DR Plan
- Oversees recovery operations
- Maintains DR documentation
- Reports to Executive Management

ICT Unit Staff

- Execute technical recovery procedures
- Restore systems and data
- Monitor recovery progress
- Document recovery actions

Department Heads

- Identify critical business processes
- Support recovery of departmental operations
- Communicate impacts to staff

All Staff

- Follow instructions during DR events
- Report incidents promptly

Third-Party Vendors

- Provide support for systems under contract
- Comply with LMHRA DR requirements
- Notify LMHRA of service outages

12.0 COMMUNICATION DURING A DISASTER

LMHRA must maintain a communication plan that includes:

- Contact lists for DR Team, vendors, and stakeholders
- Alternative communication channels (SMS, WhatsApp, backup email)
- Templates for incident notifications

- Procedures for internal and external communication

13.0 TESTING AND MAINTENANCE

- DR Plan must be tested **annually** through simulations.
- Backup restoration tests must be conducted **quarterly**.
- Test results must be documented and reviewed.
- DR Plan must be updated after:
    - Major system changes
    - Organizational changes
    - Lessons learned from incidents

14.0 SECURITY AND COMPLIANCE

- DR activities must comply with LMHRA's Information Security Policy.
- Backup and recovery data must be encrypted.
- Access to DR systems must be restricted.
- All DR actions must be logged and auditable.

15.0 POLICY VIOLATIONS

Non-compliance may result in:

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

16.0 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.

17.0 APPROVAL

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

The Disaster 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