LIBERIA MEDICINES & HEALTH PRODUCTS REGULATORY AUTHORITY

[LMHRA]

Mobile Device and BYOD Policy

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

Document Code: ICT-POL-004	**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/ACRONYMS....5
6.0 ELIGIBILITY FOR MOBILE ACCESS....5
7.0 SECURITY REQUIREMENTS FOR ALL MOBILE DEVICES....5
7.1 MANDATORY SECURITY CONTROLS....5
7.2 PROHIBITED ACTIONS....6
8. BYOD-SPECIFIC REQUIREMENTS....6
8.1 ENROLLMENT....6
8.2 MDM ENROLLMENT....6
8.3 PRIVACY CONSIDERATIONS....6
9.0 ACCESS TO LMHRA SYSTEMS VIA MOBILE DEVICES....7
10.0 USE OF MOBILE DEVICES FOR COMMUNICATION....7
11.0 LOST, STOLEN, OR COMPROMISED DEVICES....7
12.0 DATA STORAGE & HANDLING....7
13.0 PHYSICAL SECURITY....8
14.0 DEVICE DISPOSAL OR TRANSFER....8
15.0 MONITORING & COMPLIANCE....8
16.0 VIOLATIONS & ENFORCEMENT....8
17.0 POLICY REVIEW....8

18.0 APPROVAL.....9

1.0 PURPOSE

The purpose of this Mobile Device & Bring Your Own Device (BYOD) Policy is to establish clear rules for the secure use of mobile devices whether LMHRA-owned or personally owned when accessing LMHRA systems, data, or communication platforms.
This policy ensures that mobile device usage does not compromise the confidentiality, integrity, or availability of LMHRA information assets.

2.0 SCOPE

This policy applies to:

- All LMHRA staff, contractors, consultants, interns, and partners
- All LMHRA-owned mobile devices (phones, tablets, laptops, hotspots)
- All personally owned devices used to access LMHRA systems (BYOD)
- All LMHRA systems, applications, and data accessed via mobile devices
- All third-party service providers using mobile devices to access LMHRA resources

3.0 POLICY STATEMENT

LMHRA permits the use of mobile devices including BYOD under strict security controls. All users must comply with this policy to ensure that mobile access does not expose LMHRA to cybersecurity threats, data breaches, or regulatory non-compliance.

4.0 GUIDING PRINCIPLES

- **Security First** — Mobile access must not compromise LMHRA systems.
- **Least Privilege** — Access is granted only as needed for job duties.
- **Compliance** — Align with ISO 27001, Liberia Data Protection Act, and national ICT regulations.
- **Accountability** — Users are responsible for safeguarding devices and LMHRA data.

- **Separation of Personal & Official Data** — BYOD must not mix personal and LMHRA data without controls.

5.0 DEFINITIONS/ACRONYMS

- **Mobile Device:** Smartphones, tablets, laptops, USB modems, and any portable computing device.
- **BYOD:** Personally owned devices used to access LMHRA systems or data.
- **MDM (Mobile Device Management):** Security tools used to manage and protect mobile devices.
- **Sensitive Data:** Confidential or Highly Confidential information as defined in LMHRA's Data Classification Policy.

6.0 ELIGIBILITY FOR MOBILE ACCESS

- Only authorized staff may use mobile devices for LMHRA business.
- BYOD participation is voluntary and requires written approval.
- Devices must meet LMHRA security requirements before access is granted.

7.0 SECURITY REQUIREMENTS FOR ALL MOBILE DEVICES

7.1 MANDATORY SECURITY CONTROLS

All LMHRA-owned and BYOD devices must have:

- Strong password, PIN, or biometric authentication
- Auto-lock enabled after inactivity
- Up-to-date operating system and security patches
- Antivirus/endpoint protection (where applicable)
- Encryption enabled for device storage
- Screen lock and inactivity timeout

7.2 PROHIBITED ACTIONS

Users must not:

- Disable security controls
- Jailbreak or root devices
- Install unauthorized apps that pose security risks
- Store Highly Confidential data on mobile devices unless encrypted and approved
- Share LMHRA data via personal apps or cloud services

8. BYOD-SPECIFIC REQUIREMENTS

8.1 ENROLLMENT

- BYOD devices must be registered with the ICT Unit.
- Users must sign a BYOD Agreement acknowledging responsibilities.

8.2 MDM ENROLLMENT

- LMHRA may require installation of MDM tools to:
    - Enforce security settings
    - Separate personal and official data
    - Enable remote wipe of LMHRA data
    - Monitor device compliance (not personal content)

8.3 PRIVACY CONSIDERATIONS

LMHRA will not access:

- Personal photos
- Personal messages
- Personal apps
- Personal browsing history

MDM controls apply **only** to LMHRA data and configurations.

9.0 ACCESS TO LMHRA SYSTEMS VIA MOBILE DEVICES

- Access must be approved by the ICT Manager.
- Remote access must use secure VPN and MFA.
- Sensitive data must not be downloaded unless encrypted and authorized.
- Users must log out after each session.

10.0 USE OF MOBILE DEVICES FOR COMMUNICATION

- LMHRA email must be accessed only through approved apps.
- Messaging apps must be LMHRA-approved for official communication.
- Sensitive information must not be shared via SMS or unapproved apps.

11.0 LOST, STOLEN, OR COMPROMISED DEVICES

Users must immediately report:

- Lost or stolen devices
- Suspected malware infections
- Unauthorized access attempts
- Compromised passwords

ICT may remotely wipe LMHRA data from the device if necessary.

12.0 DATA STORAGE & HANDLING

- Highly Confidential data must not be stored on BYOD devices.
- Confidential data must be encrypted at rest and in transit.
- LMHRA data must not be backed up to personal cloud accounts.
- Screens must not be visible to unauthorized individuals in public spaces.

13.0 PHYSICAL SECURITY

Users must:

- Keep devices in their possession or locked securely
- Avoid leaving devices unattended in vehicles or public areas
- Use privacy screens when working in public

14.0 DEVICE DISPOSAL OR TRANSFER

Before disposal, sale, or transfer of any device:

- LMHRA-owned devices must be wiped by ICT
- BYOD users must delete all LMHRA data
- Mobile device Management (MDM) profiles must be removed by ICT

15.0 MONITORING & COMPLIANCE

- ICT may monitor device compliance with security requirements.
- LMHRA reserves the right to restrict or revoke mobile access at any time.
- Monitoring will comply with national laws and LMHRA privacy standards.

16.0 VIOLATIONS & ENFORCEMENT

Non-compliance may result in:

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

17.0 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.

18.0 APPROVAL

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

The Mobile Device and BYOD 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