Ministry of Health Republic of Liberia

Information and Communication Technology (ICT) Standard Operating Procedures (SOPs)

February 2023

1 OVERVIEW

1.1 Introduction

The Ministry of Health is the custodian and provides ICT resources to its staff and designated users in order to enhance their efficiency and productivity. These resources serve as tools with which individuals can access and process information. ICT resources in this context include desktop devices; portable and mobile devices; networks including wireless networks; Intranet and Internet connectivity; video conference facilities; door access control; CCTV; software packages/applications; external storage devices and peripherals like printers and scanners. Misuse of these resources can result in unwanted risk and liabilities.

This document reinforces the Standard Operating Procedures (SOPs) for employees and other designated users of the Ministry of Health on the use of information and communication technology (ICT) resources. Additionally, rules governing the use of specific ICT Resources are explained as are the network acceptable use guidelines.

1.2 Purpose

The purpose of the SOP document is to provide clear guidelines and instructions on how to perform routine ICT tasks and procedures in order to improve efficiency, protect ICT asset, ensure confidentiality and compliance with quality standards. It seeks to leverages MoH investment in its ICT infrastructure by defining rules that govern the lawful, consistent and appropriate use of its ICT equipment.

1.3 Scope

This SOP applies equally to all MoH employees including permanent, temporary, part-time and contract employees, as well as learners, contractors, consultants, or any other third-parties who are granted access to MoH ICT infrastructure. This includes but not limited to network, information systems, computers, associated peripherals and software.

1.4 Objectives:

i. To ensure that the MoH ICT facilities and services are used in an appropriate and responsible manner;

ii. To ensure that appropriate password controls are implemented that address the risk of unauthorized access into the variety of Information and Communication Technology (ICT) facilities and services;

iii. To safeguard the integrity and security of the MoH ICT facilities and services

2 Roles and Responsibilities

Role	Includes	Responsibilities
Senior Management	Minister, Deputies, Asst. Minister, Directors	

Supervisors	• MoH staff supervising other staff	• Oversee the acceptable use of ICT resources. • Act when they become aware of a breach of this policy. • Escalate any continuing and ongoing policy breaches. • Ensure staff are aware of their responsibilities under this policy and the consequences of inappropriate behavior.
Staff	• MoH staff: permanent, temporary and casual	• Use MoH ICT resources in accordance with this policy. • Inform supervisors when they become aware of breaches of this policy by other staff. • Report any security incidents to the appropriate channels.
Guests	• Non-MoH staff: contractors, consultants, volunteers, external partners, and international guests	• Use MoH ICT resources in accordance with this policy. • Inform supervisors when they become aware of breaches of this policy by other staff. • Report any security incidents to the appropriate channels

3 ICT Asset Acquisition

3.1 Procurement and Donations

3.1.1 All requests for ICT Asset (i.e., hardware, software, data, web domains, cloud services, etc.) after been approved by requesting department must be submitted to the ICT Unit for technical specifications and review.

3.1.2 An ICT Unit staff will be assigned to work with end-users to determine the appropriate technology (with minimum specifications) for their needs.

3.1.3 All end-users upon request for ICT Asset will be require to fill-out an **ICT Asset Request Form** which will be completed and submitted to the Department of Administration for approval.

3.1.4 All Partners donating ICT equipment to or procuring ICT equipment for any department or unit within the Ministry are must collaborate with the ICT Unit to ensure compliance with this SOP.

3.1.5 ICT Unit will review and approve specifications submitted by vendors to ensure consistency and avoid unnecessary delay in procurement.

3.1.6 Upon procurement and delivery, the ICT will receive the equipment, install and test the equipment and work with Asset Management for **Asset Coding**, fill-out the end-user receipt form before handing over the equipment to the end-user.

3.1.7 **It is a breach of this SOP should any Department, Unit or Program within the MOH procures or adopts ANY ICT Asset (i.e., hardware, software, data, web domains, cloud services, etc.) without following the procedures spelled out in this document.**

3.2 Contracts

3.2.1 ICT Unit will be responsible for the administration of technology contracts including, but not limited to: hardware, software, data, web domains, cloud services, etc.

3.2.2 The ICT Unit will be involved in all actions associated with contracts, including renewals, warranty issues, Service Level Agreements (SLAs) and vendor returns or replacement.

4 Application Development and Adoption

4.1.1 All request for software application selection process must be made to the ICT Unit through an official request for approval to the Deputy Minister for Administration Office.

4.1.2 The ICT Unit will work with the requesting unit and provide technical guidance for developing user requirement specifications including end-user desired features and functionalities.

4.1.3 The ICT Unit is the responsible lead for all software application selection, development, deployment, testing and Go-Live within the MOH.

4.1.4 The ICT Unit is responsible for the management and administration of all information systems and applications including user management, server and hosting management, backup, recovery and renewal.

4.1.5 All adopted systems and systems in development must go through proper testing by the ICT Unit and HIS Unit for each update before rollout.

4.1.6 All Units will remain only USERS and not ADMINISTRATORS of the systems for all information systems within the MOH.

4.1.7 The ICT Unit may reject an application on the follow accounts: not fit-for-purpose, lacks sustainability, non-scalable, non-interoperable with other MOH information systems and unnecessarily costly.

4.1.8 **It is a breach of this SOP should any Department, Unit or Program within the MOH procures, adopts or implements ANY software application (i.e., Database Systems, data collection tools, Cloud Platforms, etc.) without following the procedures spelled out in this document.**

5 Acceptable Use

5.1.1 MoH ICT resources are the property of the MoH and may only be lawfully used in the manner that the MoH permits.

5.1.2 You are only permitted to use ICT resources for the performance of your official duties, subject to the Personal Use clause below. All other use of ICT resources is prohibited without prior written approval.

5.1.3 Users should only access ICT resources that they have authorization to.

5.1.4 You may make reasonable personal use of some MoH ICT resources, such as email and web browsing on the desktop or laptop computer that is issued to you.

5.1.5 Password protected screen savers should be activated when a computer (desktops, laptops, mobile devices, etc.) is left unattended, or not accessed for a period of time.

5.1.6 Report harmful events or violation involving MOH ICT assets or information to their manager or ICT Unit.

5.1.7 Notify the ICT Service Desk of any leavers or changes to staff roles so that access can be terminated or amended.

6 Unacceptable Use

6.1.1 Accessing malicious contents that introduce viruses, worms, trojan horses or other harmful programs or files.

6.1.2 Installation or download of any software to any MOH ICT asset without ICT Unit guidance or approval.

6.1.3 Leave your systems (i.e., desktop, laptop, users accounts, etc.) unattended or unlock.

6.1.4 Allow personal use to interfere with or limit access to shared ICT resources

6.1.5 Access or download large personal files or unapproved software, or save them to shared ICT resources such as a network drive.

6.1.6 Use of ICT resources assigned to you for any political, commercial, personal, social or any other reason that is work related.

6.1.7 Access or share sexually explicit, obscene or otherwise inappropriate materials using ICT resources provided to you by the MOH is not allowed.

6.1.8 Unauthorized access, copy and/or dissemination of classified or sensitive information

7 Prohibited Use

7.1.1 Do not allow access to MOH ICT resources by sharing your User ID or login credentials with unauthorized individuals or partners.

7.1.2 Do not produce, download, display and circulate any offensive material in any form.

7.1.3 Do not ICT resources to send threatening or harassing messages, whether sexual or otherwise either to defame someone or for your own pleasure.

7.1.4 Do not use ICT resources to engage in any conduct that vilifies, harasses or discriminated against a person on the basis of their race, sex, sexual preference or identity, religion or disability.

7.1.5 Do not download or install application that interfere with or disrupt network resources, including propagation of computer viruses or other harmful programs.

7.1.6 Excessive personal use of ICT resources is prohibited, particularly where it impacts on your official duties or on MoH operational effectiveness, clients, staff or resources.

7.1.7 Do not use MoH ICT resources to access streaming media, create or post to personal blogs or personal web pages, or conduct a private online business (including selling on eBay or similar sites, or share trading).

7.1.8 Do not use ICT resources to engage in any unlawful conduct, including any conduct that contravenes any Liberian laws.

7.1.9 Do not use ICT resources to as a medium to infringe any intellectual property and copyright laws.

7.1.10 Do not distribute chains messages such as SPAMs using MOH Network resources.

7.1.11 Do not create, communicate, access, download or store inappropriate or prohibited material using MoH ICT resources unless.

8 Bring Your Own Devices (BYOD)

8.1.1 The use of personally own devices to connect to MOH network is a privilege granted to employees only upon formal approval by the ICT Unit.

8.1.2 All personally owned devices that connect to MOH network will be subjected to terms and conditions of this SOP or all other ICT Policies.

8.1.3 All personally owned devices that connect to MOH network will be subjected to terms and conditions of this SOP or all other ICT Policies.

8.1.4 To connect to MOH network, all personally owned devices and or workstations must have ICT Unit approved virus and spyware detection/protection software along with firewall protection active.

8.1.5 Mobile devices that access MOH corporate email must have a PIN or other authentication mechanism enabled.

8.1.6 Confidential information should only be store on personally owned devices that are encrypted in compliance with MOH ICT encryption standard.

8.1.7 Theft or loss of any personally owned devices that create, store or access MOH confidential or internal information must be immediately reported to ICT Unit.

8.1.8 Jail-broken or routed devices must not be used to connect to MOH information resources.

8.1.9 MOH ICT may choice to execute remote wipe capabilities for personally owned devices WITHOUT WARNING to the user or owner.

8.1.10 MOH ICT Support for personally owned devices is limited to assistance in compliance with this SOPs.

8.1.11 Personally owned devices may be removed from the employee's possession in the instance of a suspected incident or breach as part of a formal investigation or recovery of data.

8.1.12 All personally owned devices in relation to MOH information resources may be monitored at the discretion of the ICT Unit.

8.1.13 MOH ICT Unit reserves the right to revoke personally owned device use privileges in the event that employee do not abide by the requirement set forth in this SOPs.

9 Personal Information

9.1.1 The MoH will use employee personal information including your name, position, staff number and business contact details (email, phone, location) to provide ICT services.

9.1.2 When you voluntarily provide other information such as your personal mobile number, email address or home address to the MoH, you agree that this information may also be used to provide ICT services.

9.1.3 The provision of ICT services may entail testing, training and support of ICT systems, which may be carried out on premises or in outsourced arrangements with approved service providers.

10 Security Practices

10.1 Security Awareness

10.1.1 All users are must abide to security practices to protect MoH information and ICT resources.

10.1.2 All users are responsible for the security of ICT resources on a day-to-day basis, and must be aware of their responsibilities under this SOPs.

10.1.3 Users must read and abide by this policy for the term of your employment, contract or engagement with the MOH.

10.1.4 Users must Sign an **'Acceptable Use Agreement'** Form acknowledging that they have read this SOPs and submit their form to the ICT Unit.

10.1.5 Users are required to attend ICT security awareness training when instructed to do so by your supervisor.

10.2 Security Leadership

10.2.1 Senior Management or heads of any supported department or Unit must ensure that all external parties (partners, donors, consultants, TAs, etc.) abide with ICT security practices while engaging with the MOH.

10.2.2 All supervisors must provide leadership to help achieve good security practices, and ensure that their staff are aware of their responsibilities under this SOPs.

10.2.3 All Unit head and supervisor must ensure that staff have access to the current version of this SOP in order to access ICT resources for work.

10.2.4 All supervisors must ensure that their staff sign the Acceptable Use Agreement form and send completed forms to ICT Unit.

10.2.5 Supervisors must ensure that staff participate security awareness training when directed to do so.

10.3 Username and Password

10.3.1 Users are personally responsible for the security of their individual login details and will be held responsible for any activity carried out using their login details.

10.3.2 Passwords, PIN numbers and access codes must not be shared with anyone.

10.3.3 Password must not be written down and left visible to others, or stored on mobile devices e.g., Laptops, iPads.

10.3.4 Use a complex password or personal identity number (PIN) on all devices (e.g. laptops, tablets and smartphones) that are vulnerable to loss or theft. "Password123" or "1234567" are examples of extremely poor and easily-guessed passwords and PINs.

10.3.5 You are responsible for setting, changing, and securing your passwords in accordance with this SOP.

10.3.6 Do not reveal the passwords you know to anyone, including a supervisor or manager, ICT staff, colleagues, family, friends or strangers.

10.3.7 Do not send a password in email or other form of electronic communication (i.e. text, chat).

10.3.8 Do not type a password in a questionnaire or security form.

10.3.9 Do not use the same password or PIN for more than one user account or device.

10.3.10 If you must store a password online, ensure that it is properly encrypted using a system approved by ICT Unit.

10.4 Information and Data Security

10.4.1 Only release official information to organizations and individuals with a demonstrated "Need to Know'.

10.4.2 Apply the need-to-know principle when disseminating official information, even if you are communicating with other staff.

10.4.3 Do not disclose official information to unauthorized recipients. Authorization to disclose official information to recipients, including the public, must first be obtained from your supervisor.

10.4.4 Do not send sensitive or classified information to external parties unless it is appropriately protected (i.e., encrypted).

10.4.5 Do not send MoH information to private email accounts.

10.4.6 Immediately notify relevant Unit (information owner) within the MOH if you receive official information (i.e., email messages, attachments, etc.) that is not intended for you. Such information will be deleted from the user's device.

10.5 Physical Security

10.5.1 Lockup computers when not in use to prevent unauthorized access or theft. (theft or loss)

10.5.2 If the computer is shared, you must log off the computer before it is used by others.

10.5.3 Do not download, install or run unauthorized security programs or utilities which reveal weaknesses in the security of a system.

10.5.4 All users are responsible for the physical security of ICT assets assigned to them (Field Work)

11 Network Access

11.1 Access to Internet and Intranet

11.1.1 Users access to internet service within the MOH will be given to employees based on their job description, roles and responsibilities.

11.1.2 Access to internet should be requested through Unit/Programs heads.

11.1.3 All users will be given credentials by the IT Unit to access network resources within the MOH.

11.2 Access to Wireless Network

11.2.1 Users must register the access device and obtain approval from the ICT Unit before connecting the access device to the Government wireless network.

11.2.2 Wireless client systems and wireless devices shall not be allowed to connect to the MoH wireless access points without due authentication.

11.2.3 All staff shall **register** their client system and obtain approval from the ICT Unit before connecting the client system to the MoH network.

11.2.4 Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

11.2.5 To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

•

11.3 Network and Local Drives

11.3.1 Do not save software and/or large personal files to any network drive or assigned computer hard drive.

11.3.2 Avoid as much as possible personalizing MOH assigned equipment.

12 Email and Electronic Communication

12.1.1 Employees should not use personal email accounts to send or receive MOH confidential information.

12.1.2 For official communication employees must use their assigned corporate email accounts.

12.1.3 Use caution when responding to, clicking-on links within or opening attachments included in electronic communication.

12.1.4 Avoid opening attachments and clicking on links when content is not adequately explained (e.g., "Watch this video, it's amazing.")

12.1.5 Be suspicious of clickbait titles.

12.1.6 Check email and names of unknown senders to ensure they are legitimate.

12.1.7 Look for inconsistencies or style red flags (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

12.1.8 Avoid opening email that carry malware and phishing attempts.

12.1.9 Do not forward or reply to any spam message (i.e., unsolicited commercial email).

12.1.10 Do not auto forward electronic messages outside the MOH internal system (Intranet or corporate email system).

12.1.11 Employees should use their corporate email accounts to attending virtual meetings for proper identification.

12.1.12 Do not use corporate email accounts to engage in distribution of unauthorized emails (i.e., bulk email or chain message) that seek personal gain, encourages industrial action and supports political purposes.

12.1.13 Report all unauthorized emails receive from any employee through your corporate email account to your supervisor or the ICT Unit.

12.2 Cloud services

12.2.1 Do not engage cloud service providers who do not comply with the MoH and Liberian law.

12.2.2 Do not engage a cloud service provider for official purposes without approval from the ICT Director or their delegate.

12.2.3 Reasonable personal use of cloud services is permitted, provided it is not **prohibited use** as defined by this SOP.

12.2.4 Do not transfer official information to a cloud service provider without approval from the ICT Unit.

13 Software

13.1 Copying or Installing Software

13.1.1 Do not copy or install software on MoH computers unless you have obtained prior approval to do so from the ICT Unit.

13.1.2 This applies to all software, including software that is privately owned or obtained from the Internet, online services or portable media such as CD/DVD or USB key.

13.2 Malicious Software

13.2.1 Content that is intentionally or accidentally downloaded from websites or received by email may contain malicious software ("malware") such as viruses.

13.2.2

13.2.3 All MoH computers have anti- virus software installed to automatically check downloaded files, but this is not a guaranteed to identify all malware.

13.2.4 Do not to download untrusted content from websites or removable media to an MoH computer.

13.2.5 When it is necessary to download files, only do so from known or trusted sources.

13.2.6 Be cautious when opening email attachments, especially you do not know the sender, or if the sender is not an MoH staff member.

13.2.7 Avoid visiting compromised websites that harbor malware. They can be hard to tell at a glance, but Internet Explorer, Google Chrome, and Mozilla Firefox is configured to warn MoH users before downloading potentially unsafe content. Pay attention to these warnings.

13.2.8 If you suspect an ICT resource has been infected with malware (e.g., a warning is displayed, or your computer behaves erratically or runs very slowly), contact the ICT Unit immediately.

14 Copyright and Intellectual Property

14.1.1 Material accessible through the MoH's network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information.

14.1.2 Users shall not use the MoH network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

15 Reporting

15.1 Reporting Offensive Material

15.1.1 Report any message you believe is offensive, humiliating or intimidating that you reasonably believe was deliberately sent to you.

15.1.2 Report these incidents to your immediate supervisor or to the ICT Unit. All complaints will be addressed promptly and treated impartially and confidentially.

15.2 Security Incident Reporting

15.2.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of MoH data. All staff must report security incidents to the appropriate channels (Table 1) as soon as possible. This applies to incidents that are personally detected by you or are referred to you, for example, by a customer or an external organization.

15.2.2 MoH reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system.

15.2.3 Do not discuss security incidents with media, the public or staff outside these reporting channels, unless authorized to do so by a delegate.

16 Compliance

16.1 Logging and Monitoring

16.1.1 ICT Unit will maintain logs, backups and archives of activities on all ICT resources including computers, laptops, smartphones and tablets

16.1.2 ICT Unit will monitor email server performance and retention of logs, backups and archives of emails sent and received through MoH servers

16.1.3 ICT Unit will retain logs, backups and archives of all Internet access and network usage.

16.1.4 ICT Unit will not disclose the contents of monitoring to a person, body or management unless one or more of the following applies:

16.1.4.1 The staff member is reasonably likely to have been aware, or made aware that information of that kind is usually passed to that person, body or Senior Management

16.1.4.2 ICT Unit believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person

16.1.4.3 Senior Management has requested monitoring or investigation

16.1.4.4 The disclosure is required or authorized by or under law

16.1.4.5 The disclosure is necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue

16.2 The ICT Unit may log computer activity:

16.2.1 for system management and planning

16.2.2 to ensure compliance with MoH policies

16.2.3 to investigate conduct that may be illegal or adversely affect MoH staff

16.2.4 to investigate inappropriate or excessive personal use of MoH ICT resources

16.3 Password Auditing

16.3.1 ICT Unit may audit passwords to assess and enforce compliance with this SOP. Password audit results are reviewed by the ICT Director or his/her designated person/s.

16.4 Investigations

16.4.1 ICT Unit can access and monitor the logs of all staff activity including the URLs or website ICT addresses of sites visited, the date and time they were visited and the duration of site visits and logs for the purpose of investigating breaches of this SOP.

16.4.2 ICT unit will access and monitor email messages and attachments, including backups and archives of emails, whether they are current or have been deleted by the user for the purpose of investigating breaches of this SOP

16.4.3 ICT Unit in consultation with Senior Management may authorize the investigation of user logs in the event that there is a perceived threat to MoH ICT system security, the privacy of MoH staff, the privacy of others and legal liability of the MoH.

16.4.4 These records can be called up and cited as a chain of evidence in legal proceedings and actions following virus attacks. Access will be fully logged and documented.

17 System Access Control

17.1.1 System Access Control refers to the process that regulates who or what can view or use ICT resources. It is a fundamental concept that minimizes risk to the Ministry of Health (MOH).

17.1.2 The privileges of all users, systems, and independent operating programs such as agents, must be restricted based on role.

17.2 Limiting System Privileges

17.2.1 Default user file permissions must not automatically permit anyone on the system to read, write, execute or delete a system file.

17.2.2 Default file permissions granted to limited groups of people who have a genuine need to know are permitted.

17.2.3 All users with BYODs must have a lock screen.

17.2.4 MOH computer and communications systems must restrict access to computers that users can reach over MOH networks through a firewall and filter.

17.3 Process for Granting System Privileges

17.3.1 Requests for new user IDs and changed privileges must be in writing and approved by the user's supervisor before a system administrator fulfills these requests.

17.3.2 Non-MOH employees, students, or partners will require written approval from Senior Management to access MoH systems.

17.3.3 Non-MOH employees requesting access to MOH systems will be provided access for a period not more than 30 days.

17.3.4 Access to read/write to the files of other users, will be approved by the systems administrator or owner of the files.

17.3.5 Configuration changes, operating system changes, and other related activities that require high level system privileges must be performed by system administrators (ICT Unit).

17.3.6 All users that connect to MOH internal networks or systems signify their agreement to comply with all applicable SOPs by their logon to the network.

17.4 Revoking System Access

17.4.1 All user IDs should have the associated privileges revoked after a period of inactivity not exceeding 180 days (6 months).

17.4.2 If any MoH system or equipment is malfunctioning, it should default to denial of privileges to users.

17.4.3 If access control subsystems are malfunctioning, the systems will remain unavailable until the problem has been rectified.

17.4.4 Unless specifically approved in advance in writing by the ICT Unit Director, users must not test computer or communication system security measures.

17.4.5 Unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise MoH security measures is unlawful and in violation of MOH policy.

17.4.6 The privileges granted to MoH employees should be reevaluated by administration annually and revoke all necessary privileges no longer needed by said employees.

17.4.7 For all terminations/transfers/resignations, the Human Resources department must issue a notice of status change to the ICT Unit.

17.5 Establishment of Access Paths

17.5.1 Employees must not establish electronic bulletin boards, local area networks, FTP servers, web servers, illegal Peer-to-Peer sharing or other multi-user systems for communicating information without the specific approval of the ICT Unit Director.

17.5.2 Portable devices (smartphones, tablet computers, etc.) using WIFI or commercial data networks should not be used for data transmissions containing confidential personal information unless the connection is encrypted.

17.6 End-User Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Ministry's network and data. As such, all employees, partners, researchers, students with access to MOH systems are responsible for selecting and securing their passwords as outlined below.

17.7 Password Creation Guidelines

17.7.1 The password must be at least 13 characters in length. (Longer is generally better.)

17.7.2 The password should not be a word in the dictionary

17.7.3 The password must be in mixed case (upper- and lower-case letters)

17.7.4 The password must contain at least one numeric character.

17.7.5 The password cannot be the same as the user ID.

17.7.6 Special characters may be used to strengthen the password. Examples of permitted special characters are $.,! % ^ *

17.7.7 The password should not be information easily obtainable about you such as your license plate number, date of birth, social security number, telephone number, or address.

17.8 Password Protection

17.8.1 Passwords stored electronically may not be stored in readable form or written down and left in a place where unauthorized persons might discover them.

17.8.2 Passwords may never be shared or revealed to anyone other than the authorized user.

17.8.3 If a password is suspected of being disclosed or known to have been disclosed to anyone other than the authorized user, it should be changed immediately.

17.8.4 Passwords will expire quarterly - every 90 days. When a password expires or a change is required, users should create a new password that is not identical to the last three passwords previously used.

17.9 Password System Set-Up

17.9.1 All computers permanently or intermittently connected to MOH local area networks (LAN) must have password access controls. If the computers contain confidential or protected information, an extended user authentication system approved by the ICT Unit must be used.

17.9.2 Multi-user systems (servers) should employ user IDs and passwords unique to each user, and user privilege restriction mechanisms with privileges based on an individual's need to know.

17.9.3 Network-connected, single-user systems must employ hardware or software controls approved by ICT Unit that prevent unauthorized access.

17.9.4 All vendor-supplied default fixed passwords must be changed before any computer or communications system is used by end-users.

17.9.5 After five unsuccessful attempts to enter a password, a reset may be required by a system administrator (ICT Unit) or temporarily disabled for no less than three minutes.

17.9.6 In the event a system has been compromised, the system administrator must notify all end-users of said system and reset all users' passwords.

17.10 Equipment Control

17.10.1 Computers, BYOD, mobile devices (smartphones and tablets), modems, wireless access points, routers, switches or other devices connected to MOH ICT Infrastructure are forbidden unless

they meet all technical requirements and have a user authentication system approved by the ICT Unit.

17.10.2 All MOH owned ICT equipment must be coded by Assets Management before assignment and use.

18 Logon and Logoff Process

18.1 Logon

18.1.1 All users must be positively identified (Unique user ID and password) prior to being able to use any MoH ICT system or hardware.

18.1.2 If logon is unsuccessful, please contact the ICT Unit.

18.2 Logoff

18.2.1 All users must log off when not using ICT systems or hardware.

18.2.2 If there is inactivity on any MoH ICT system or hardware for more than 10 minutes, the system should automatically logoff the use and terminate the session.

18.3 Anonymous Logon

18.3.1 Users are strictly prohibited from logging into any MOH system or equipment anonymously.

19 Software and Backup

19.1 Software

19.1.1 All MOH purchased software should be copied prior to its initial usage, and such copies must be stored in a safe place.

19.1.2 MOH computers and networks must not run software that comes from sources other than business/academic partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors.

19.2 Storage and Backup

19.2.1 For multi-user computer systems, whenever systems software permits, backups must be performed without end-user involvement, over an internal network and during the off hours.

19.2.2 Personal computer users are responsible for backing up the information stored on their local machines.

19.2.3 Multi-user computer (servers) and communication systems, a system administrator is responsible for making periodic backups.

19.2.4 Storage of backup media is the responsibility of the office computer user or servers' system administrator.

19.2.5 Backup media should be stored in fireproof safes, at a separate location away from the system being backed up.

19.2.6 Whenever Confidential information is written to a disk or other storage media, the storage media should be suitably marked with as such.

19.2.7 Directors are responsible for preparing, testing and periodically updating department contingency plans to restore service for all non-IT managed production applications and systems.

19.2.8 All confidential information stored on backup media should be encrypted using approved encrypting methods.

20 Portable Equipment

20.1.1 Employees in the possession of portable, laptop, notebook, handheld, tablet and other transportable computers containing confidential information must not leave these computers unattended at any time.

21 Remote Printing

21.1.1 Printers must not be left unattended if Confidential information is being printed or soon will be printed.

21.1.2 Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

22 Privacy

22.1.1 Unless contractual agreements dictate otherwise, messages sent over MOH computer and communications systems are the property of Ministry of Health and the Republic of Liberia.

22.1.2 Personal Data Privacy: Administration reserves the right to examine all data stored in or transmitted by MoH systems or equipment.

22.2 Encryption

22.2.1 All protected/confidential files/documents must use 128-bit password-based encryption.

22.2.2 Systems and application storage of end-user's passwords must be encrypted.

23 Logs and Other Systems Security Tools

23.1 Minimum Computer & Network Security

23.1.1 Every server or communication system must include mechanisms for the recording, detection, and correction of commonly-encountered security problems.

23.1.2 Automated tools for handling common security problems must be used on MOH computers and networks.

23.1.3 Computer and communications systems handling sensitive, valuable, or critical MOH information must securely log all significant security relevant events.

23.2 Computers Logs

23.2.1 Logs containing computer or communications system security relevant events must be retained for at least three months.

23.2.2 Only system administrators (ICT Unit) are authorized to read computer logs.

23.2.3 Any modifications to MoH systems and equipment logs are strictly prohibited.

23.3 Software Patches

23.3.1 System administrators are required to promptly apply all security patches to the operating system and relevant applications.

24 Handling Network Security Information

24.1 Compliance & Reporting

24.1.1 Every user must promptly report any suspected network security problem, including intrusions to the ICT UNIT Director or his/her designee.

24.1.2 Provided that no intent to damage MOH systems existed, if users report a computer virus infestation immediately after it is noticed, even if their negligence was a contributing factor, no disciplinary action should be taken.

24.1.3 All network or systems software malfunctions must be reported immediately to the ICT Unit or the involved external service provider.

24.1.4 Information about security measures for MOH computer and communication systems is confidential and must not be released to people who are not authorized users of the involved systems unless the permission of the ICT UNIT Director has been obtained. For example, publishing system access information in directories is prohibited.

25 Physical Security of Equipment

25.1.1 Physical security is the protection of hardware, software, networks and data from physical actions and events that could cause serious loss or damage to the Ministry's system.

25.1.2 All MOH network equipment must be physically secured.

25.1.3 Access to data centers, telephone wiring closets, network switching rooms, and other areas containing confidential information must be physically restricted.

25.2 Offsite Security

25.2.1 All employees who must keep Confidential MOH information offsite in order to do their work must possess lockable furniture for the proper storage of this information. At the time of separation from MOH, all Confidential information must be returned immediately.

26 Information Security

26.1 Risk Identification

26.1.1 All units must identify and catalog all information assets.

26.1.2 Identify threats and vulnerabilities through security audits

26.1.3 Implement internal controls with support from the ICT Unit

26.2 Employee training

26.2.1 The ICT Unit will coordinate with Human Resource to evaluate the effectiveness of the Ministry's procedures and practices relating to access to and use of confidential information and design and implement relevant training sessions with employees.

26.3 Information Systems and Information Processing and Disposal

26.3.1 The ICT UNIT Director will assess the risks to confidential information associated with the Ministry's information systems, including network and software design, information processing, and the storage, transmission and disposal of confidential information.

26.4 Monitoring Procedures

26.4.1 The ICT Unit will develop and implement procedures for monitoring potential information security threats associated with software systems.

26.4.2 Systems patches download and update including other software fixes designed to deal with known security flaws will be done ONLY by ICT Unit.

26.4.3 The ICT Unit will evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies.

26.4.4 The ICT Unit is responsible to monitoring and dissemination of information related to the reporting of known security attacks and other threats to MOH network and systems.

27 Exemptions

27.1.1 Where research and investigations are proposed or undertaken that would be likely to breach this Policy, the purpose, scope and design of work being undertaken may require prior approval through the ICT Policy Waiver Process. Ask your supervisor or the ICT Director.

28 Consequences

28.1.1 MoH ICT resources support many crucial activities for the MoH environment, including hospitals and emergency services. The ICT Unit will take all legally allowed steps it deems appropriate to remedy or prevent activities that endanger the safety of those ICT resources.

28.1.2 Breach of this SOP may constitute misconduct under the MoH Employee Handbook. Disciplinary action can include counselling, formal warning, conditions placed on continuing service, deductions from salary, changes to employment contract or termination of engagement.

28.1.3 Evidence of prohibited activities will be provided to law enforcement as soon as they are detected. Depending on the severity of the offence, suspects could be placed under arrest and prosecuted under Liberian law.

29 Review

29.1.1 Future changes in this Policy, as deemed necessary, shall be made by the ICT Unit with the approval of the Minister of Health and MoH Senior Management Team.

Ministry of Health Republic of Liberia

ICT ASSET REQUISTION FORM

Requesting Department/Unit:

Approved (Head of Department/Unit):

Date:

Type/Description (Laptop, Desktop, Smart Phone, Tablet, Printer, Copier, etc.) of equipment requested:
Reason/ justification for Purchase:
Purpose (Specific work equipment will be used for i.e., clerical work data processing and analysis, engineering basic office use, etc.)
Budget Line: GOL or Partner (please indicate line item): Estimated Budget:
Is this Request for replacement of existing equipment: Yes/No Reason for Replacement: Has the previous equipment been assessed and returned to ICT Unit: Yes/No Date of Return to ICT:
Name of staff (end-user):
Request Received By (ICT Staff):
Sub-project for costs (if not School Equipment Budget 125152-01):

NOTE: All equipment donated to or purchase by the MOH through GOL, donor or partner funding remains the property of MOH until it is formally disposed of.

Please submit completed forms to: ICT Unit, Room 234, Ministry of Health Central Office Congo Town.

Ministry of Health Republic of Liberia

ICT Acceptable Use Agreement

I, ...

(PRINT FULL FIRST, MIDDLE & SURNAME – BLOCK LETTERS and in INK)

(a) acknowledge that I have read and understood the Ministry of Health Information Communication Technology (ICT) Standard Operating Procedures (SOP)

(b) agree to abide by the requirements for access and use of these resources

(c) acknowledge that the Ministry of Health may access my user logs in the event that there is a perceived threat to the:

- System security
- Privacy of staff
- Privacy of others
- Legal liability of the Ministry of Health

This signed acceptance is valid for the period of my employment with the Ministry of Health, or until a revised statement is deemed necessary by the Ministry.

Signature: .....

Date: .....

Unit: .....

Position: .....

Employee Number: .....

Note: *Your full name must match personnel records from Human Resources. Do not use abbreviated or nicknames unless it is your formal name. Please deliver this form to the ICT Unit of the Ministry of Health Central Office.*