# FEDERAL MINISTRY OF HEALTH


## INFORMATION COMMUNICATION TECHNOLOGY

## EXECUTIVE OFFICE

## ICT POLICY AND GUIDELINES

JAN, 2024

## Contents

# Executive Summary

The Ministry of Health (MOH) ICT Policy serves as a strategic framework for managing, securing, and optimizing information and communication technology (ICT) infrastructure within the ministry. This policy establishes guidelines and procedures to ensure the efficient, secure, and reliable use of ICT in delivering services, supporting decision-making, and enhancing digital transformation within the ministry.

The policy outlines specific directives on network security, system authentication, data encryption, firewall deployment, and cyber security incident response. It also provides clear guidelines on ICT equipment disposal, website management, software development, and surveillance system protocols. Additionally, the policy emphasizes compliance, accountability, and the enforcement of ICT best practices to mitigate risks and enhance service delivery.

By implementing this policy, the MOH aims to establish a resilient, efficient, and secure ICT environment that supports the ministry's mission of delivering high-quality services through innovative technology solutions.

## Acronyms

MOH - Ministry of Health

ICT - Information communication technology

NSP - **Network Security Policy**

LAN - Local Area Network

OS - Operating System

CIA - confidentiality, integrity, and availability

IDPS - Intrusion detection and prevention systems

VPN - Virtual Private Network

ICT EO -- Information communication technology Executive Office

## Definition of Terms

**Access Point: -** Electronic hardware that serves as a common connection point for devices in a Wireless network. An access point acts as a network hub that is used to connect segments of a LAN, using transmits and receiving antennas instead of ports for access by multiple users of the wireless Network.

**Archive: -**The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room

**AUP:** An Acceptable Use Policy, also sometimes acceptable usage policy or Fair Use Policy, is a set of rules applied by the owner/manager of a network, website or large computer system that restrict the ways in which the network site or system may be used.

**Backup: -** Saving a copy of files onto mass storage media such as storage servers, hard disks or CD/DVD for the purpose of preventing loss of data in the event of disaster or destruction.

**Database: -** A file or file system containing organized information and, most commonly, a filing and retrieval system for storing information. Most database software also includes tools for data analysis. Examples of database software include Oracle, MS-SQL, My-Sql, and Microsoft Access.

**Disaster: -** Any event that might bring damage on the data storage medium. Disaster can be natural or artificial, such as fire, thunder, flood, data deletion, system failure, medium failure, and attack (from malicious scripts, viruses and others).

**Hardware: -** Hardware is a general term for the physical artifacts of a technology. It may also mean the physical components of a computer system, in the form of computer hardware.

**IT Support: -** Is defined as responses to any queries made by end users to IT regarding failures, problems, issues, questions, and other matters relating to the operation and continuity of MoH's ICT services.

**Junk Email: -** E-mail spam, also known as junk e-mail, is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. A common synonym for spam is Unsolicited Bulk E-mail (UBE). Definitions of spam usually include the aspects that email is unsolicited and sent in bulk. "UCE" refers specifically to Unsolicited Commercial E-mail.

**Network: -** Computer systems and connecting devices connected together using telecommunication for the purpose of communicating and sharing resources in MoH's compound.

**Local Area Network (LAN**):- is a network infrastructure whose span is limited to the MoH's Compound.

**Security: -**Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

**Server: -** is a computer program that provides services to other computer programs (and their users) in the same or other computers. The computer that a server program runs in is also frequently referred to as a server. That machine may be a dedicated server or used for other purposes as well.

**Spam: -** in particular e-mail spam, is unsolicited or undesired electronic bulk messages sent through email with commercial, fraudulent or malicious intent.

**Software: -** Computer software is often regarded as anything but hardware, meaning that the "hard" are the parts that are tangible while the "soft" part is the intangible objects inside the computer. Software encompasses an extremely wide array of products and technologies developed using different techniques like programming languages, scripting languages, micro-code, etc.

**User: -** Any employee, consultant or guest in MoH who uses MoH's ICT infrastructure and services for office work. It includes users of the Internet, applications, database systems or the ICT infrastructure.

**Office Applications: -** In computing, an office suite, sometimes called an office software suite or productivity suite is a collection of programs intended to be used by knowledge workers. The currently dominant office suites are Microsoft Office, which is available for Microsoft Windows and Apple Inc.'s Mac OS X, and OpenOffice.org, free software (open source alternative) available for many operating systems.

**Operating System: -** Software that controls a computer and acts as a layer between the hardware and the applications and users. (e.g. Linux, Windows, Mac OS X, UNIX).

**Restore: -** The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

**Wireless Network: -** Refers to any type of computer network that is wireless, and is commonly associated with a telecommunications network whose interconnection between nodes is implemented without the use of wires.

# 1. INTRODUCTION

Information communication technology is an inclusive term that refers to technologies which are being used for collecting, storing, editing and passing on information in various forms. The importance of ICTs is not the technology as such, but it's enabling function in facilitating enhanced access to information and communication across large distances. ICTs have been used in many innovative ways to achieve social impacts, such as promoting access to basic services.

The purpose of this document is to create a policy for all employees and management of the Ministry of Health appropriate use, procurement, software development, web site administration, network security, data retention, personal use, internet & email, support services, training, etc. This policy will be reviewed annually to incorporate changes in policy due to changes in technology.

## 1.1. Objectives

The main objectives of the MOH ICT Policy are:

- Reviewing challenges and barriers for the implementation of ICT policy
- Enhance the proper IT service utilization and minimize the challenges in IT Support
- Ensure that MOH ICT infrastructure and capacity are utilized effectively
- Provide a framework that will enable ICT to contribute towards achieving MOH goals.
- Establish a trusted and secure information infrastructure and a culture of cyber security at all levels of MOH society.
- Enhance the exploitation of ICT across MOH for increased Productivity and efficiency; and Transform MOH into an Information-based society where everyone has equitable and affordable access to ICTs and use ICT as tool for its Decision.

1.2. Scope of ICT policy

This policy and guidelines apply to the organization's information assets, which consist of information and information processing facilities and to all internal employees and relevant external parties that have access to the organization's information system resources at any level.

# 2. Data Backup and Recovery

2.1. Overview

The purpose of this policy and guidelines is to ensure that the Ministry's data backup and recovery can quickly recover from an incident and continue with its mission, a *Data Backup and Recovery Policy* must be put into place. A key part of a backup policy involves steps and methods to take backups to be prepared in case data is damaged or lost.

2.2. Purpose

Proper planning will help ICT EO recover from different types of cyber security events or natural disasters on time. This *Data Backup and Recovery Policy* provide an overarching strategy for governing the backup and recovery of data within the MOH. This includes creating a detailed data recovery process to ensure data is backed up on the correct assets. This process should be documented and quickly available in case incident occurs additionally procedures for securely protecting data from unauthorized access or modification alongside appropriate methods for how users should handle their data during their day-to-day work activities.

2.3. Policy Statement

- The ICT EO will be responsible to take the back up of data or applications configured at the FMOH data center
- It is the responsibility of the directorates or individuals for the data stored on their personal computers and the ICT EO will not be liable for any kind of data loss or corruption
- When there is a full or partial loss of data, it will restored from the most recent backups and if there is a data element not taken the backup between

the backup periods and the data loss, it is the responsibility of the data owners to reenters that portion of data.

- The ICT EO should guarantee a minimum mean time between failure(MTBF) to restore the data on its previous state

2.4. Guidelines

- Backups are taken over night or during non-working hours of the day
- The frequency and type (incremental/full backup) is determined on the type and criticality of the data
- Full backups are taken weekly whereas incremental backups are taken daily
- Back-up data will be stored in secured places and only authorized people will have access to it
- The ICT EO along with the data owners prepares a guideline setting the principles on how the backups and restoration process will take place
- Backup data should be tested periodically for its integrity to guarantee full recovery in case of data loss or damage
- Backups must have at a minimum identifying criteria like System name, creation date that can be readily identified by labels

### 2.4.1. Timing

The timing and frequency of the backups will depend on the sensitivity of data held and the potential of threats on the data. There will be a standard classification of risks for all the data and ICT infrastructure of the FMOH and based on that the timing for taking back up of each kind of resource will be determined

### 2.4.2. Storage

- After the backups are completed based on their schedule, the backup media will be stored in a secure place
- The ICT EO will configure a separate storage server to store all the backups

### 2.4.3. Recycling

Backups performed shall be kept for one month and used again the next month on the applicable date

### 2.4.4. Responsibility

- The ICT EO will be responsible to take the backup and restore in case of data loss of all applications deployed at the FMOH data center
- Individual data of employees will not be backed up by the ICT EO and it is the responsibility of the respective individual to take backup of critical work related data either on external hard disk or DVD/VCD
- The ICT EO will assign responsible experts for data backup and restoring

### 2.4.5. Testing

Backup data will be tested at least once in a month to ensure its integrity and the ability to fully restore data in case of data loss

### 2.4.6. Data and Systems to Be Backed Up

- Data to be backed up include all data of applications deployed at the FMOH data center
- Systems to be backed up are image copy of active directory, domain servers mail servers, and antivirus servers and other

### 2.4.7. Archives

Archives are made at the end of every year in June (Sene). User account data associated with the file and mail servers are archived one month after they have left the organization

### 2.4.8. Restoration

Directorates or Users that need files to be restored must submit a request to the ICT EO by providing information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

# 3. Security

3.1. Overview

The purpose of this policy and guidelines is to ensure secure and reliable IT infrastructure access and performance for MOH community. This policy and guidelines are intended to protect the IT infrastructure and mitigate the risks and losses associated with security threats to the network and information systems.

The first step towards enhancing FMOH's security is the introduction of a precise yet enforceable security policy, informing staff on the various aspects of their responsibilities, general use of resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

3.2. Policy Statements

- The ICT EO will be responsible to take the back up of data or applications configured at our data center
- It is the responsibility of the directorates or individuals for the data stored on their personal computers and the ICT EO will not be liable for any kind of data loss or corruption
- When there is a full or partial loss of data, it will be restored from the most recent backups and if there is a data element not taken the backup between the backup periods and the data loss, it is the responsibility of the data owners to reenters that portion of data.

- The ICT EO should guarantee a minimum mean time between failure (MTBF) to restore the data on its previous state

3.3. Guidelines

### 3.3.1. Physical Security

Access to secure areas, including server rooms shall be restricted to authorized staff using passwords, locks or access-control devices. Hence,

- Visitors to such areas shall be permitted only under the supervision of authorized ICT EO staff. Details of visitors including name, time in, time out, and reason for entry shall be recorded in a log.

- During non-working hours, secure areas shall be protected against intrusion by appropriate access control, surveillance systems or by security staff.
- Appropriate smoke and fire detection, alarm and supervision equipment should be provided and suitably placed.
- ICT EO has the responsibility to protect equipment from power failure and other disruptions
- ICT EO has the responsibility to check supporting utilities such as electricity, water supply, heat /ventilation and air conditioning should be adequate for systems they are supporting.
- Backup generator should be considered if processing is required to continue when power failed for longer period.
- ICT EO has the responsibility to check for UPS equipment and generators regularly and ensure they have adequate capacity and test in accordance with manufacturer recommendation.

### Cabling

The following are the responsibility of ICT EO regarding cabling:

- Check Power and telecommunication lines running underground.
- Protect network cabling from unauthorized interruption or damage.
- Prepare documented patch list of network cabling and detailed cabling diagram to enable proper cable fault troubleshooting prepare to reduce the possibility of handling error.

### 3.3.3. Maintenance of Equipment

ICT EO has the responsibility to check the following during IT related maintenance, Disposal and removal of equipment

- Only authorized maintenance personnel should carry out repairs and service equipment.
- Equipment's are maintained in accordance with the supplier's recommended Service interval and specification.
- Appropriate control is set when equipment is scheduled for maintenance taking in to account weather this maintenance is performed by personnel on site or external to the FMOH.
- Equipment, information or software should not be taken off-site without authorization.

### 3.3.4. Storage Media Handling

In this context storage media refers any permanent storage devices.

ICT EO has the following responsibilities about any media.

- Media containing sensitive information are stored and kept securely and safely within the FMOH.
- Identify Medias that might require secure disposal.
- Access to media containing sensitive information is restricted to prevent access from unauthorized personnel.
- Media containing sensitive information about system documentation are securely stored.
- System documentation stored in internal network or distributed via a public network;

- ICT EO should arrange training for personnel using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that should be implemented.

# 4. Network Security (NSP)

4.1. Overview

A network security policy is a formal document that outlines the rules and procedures for protecting an organization's computer network from unauthorized access, use, disclosure, disruption, modification, or destruction a network security policy is a living document and should be regularly reviewed and updated to reflect changes in the organization's needs, technology, and the threat landscape.

4.2. Purpose

A network security policy is a set of standardized practices and procedures that outlines rules, network access, the architecture of the network, and security environments, as well as determines how policies are enforced. It outlines the principles, guidelines, and procedures for securing the organization's network infrastructure, and ensuring the confidentiality, integrity, and availability of network resources. Videos an overarching strategy for governing the backup and recovery of data within the MOH. This includes creating a detailed data recovery process to ensure data is backed up on the correct assets. This process should be documented and quickly available in case incident occurs additionally procedures for securely protecting data from unauthorized access or modification alongside appropriate methods for how users should handle their data during their day-to-day work activities.

4.3. Policy Statements

a) The FMOH Network Infrastructure is owned by and the property of ICT EO.
b) ICT EO shall be primarily responsible for overseeing the operations of the Network Infrastructure.
c) ICT EO shall avail appropriate network infrastructure, network services & resource access to every user in the FMOH.

d) ICT EO will make available Internet access to all in the compound for users to support their tasks and solely to perform their jobs and professional roles

## 4.4. Guidelines

### 4.4.1. Assigned Network Addresses

a) Users are only permitted to use network addresses assigned to them by the Ministry's ICT Department.

### 4.4.2. Remote Access

a) All remote access to Ministry systems must occur via a secure VPN connection on a Ministry-owned device equipped with up-to-date anti-virus software.

b) Alternatively, remote access is allowed on approved mobile devices, as per the guidelines outlined in the Ministry Owned Mobile Device Acceptable Use and Security Policy and the Personal Device Acceptable Use and Security Policy.

### 4.4.3. Approved Protocols

a) Remote users may only connect to the Ministry's Information Systems using protocols approved by the ICT EO.

b) Users within the Ministry firewall are prohibited from connecting to the Ministry network simultaneously with a remote connection to an external network.

#### 4.4.4. Physical Security

Access to secure areas, including server rooms shall be restricted to authorized staff through the use of passwords, locks, or access-control devices. Hence,

a) Visitors to such areas shall be permitted only under the supervision of authorized ICT staff. Details of visitors including name, time in, time out, and reason for entry shall be recorded in a log.
b) During non-working hours, secure areas shall be protected against intrusion by appropriate access control, surveillance systems, or security staff.
c) Critical information and information processing facilities should be physically protected against man-made attacks and natural accidents on a 24/7 basis.

#### 4.4.5. Network Hardware and Software Installation

a) Users must not extend or re-transmit network services by installing routers, switches, hubs, or wireless access points to the Ministry network without prior approval from the Ministry's ICT.
b) Installation of network hardware or software that provides network services is strictly prohibited without explicit approval from the Ministry's ICT.
c) Non-Ministry computer systems requiring network connectivity must also receive approval from the Ministry's ICT or connect to the guest network, and staff members are prohibited from sharing passwords.

#### 4.4.6. Security Programs and Utilities

a) Users must refrain from downloading, installing, or running security programs or utilities that reveal vulnerabilities in the security of the Ministry's systems.
b) Examples of prohibited programs include password-cracking tools, packet sniffers, network mapping tools, and port scanners.
c) Only the ICT EO is authorized to conduct such activities for security assessment purposes.

4.4.7. Access Control

a) All network access must be controlled and restricted based on the principle of least privilege, ensuring that users have access only to the resources necessary for their role.
b) Access to sensitive network resources, such as servers and databases, must be granted on a need-to-know basis and strictly monitored.

4.4.8. Authentication and Authorization

a) Strong authentication mechanisms must be implemented for accessing critical network resources.
b) Authorization policies must be enforced to verify the identity and permissions of users and devices accessing the network.

4.4.9. Data Encryption

a) All sensitive data transmitted over the network must be encrypted using industry-standard encryption protocols to prevent unauthorized access and interception.
b) Encryption must be applied to data both in transit and at rest, including emails, file transfers, and stored data on servers and endpoints.

4.4.10. Firewall Deployment Configuration

a) Firewalls must be deployed at network boundaries to monitor and control incoming and outgoing traffic, enforcing security policies and blocking unauthorized access attempts.
b) Firewall rules must be regularly reviewed and updated to adapt to changing network requirements and emerging threats.

4.4.11. Intrusion Detection and Prevention

a) Intrusion detection and prevention systems (IDPS) must be deployed to monitor network traffic for suspicious activity, identify potential threats, and take immediate action to block or mitigate attacks.
b) Regular tuning and configuration of IDPS rules are necessary to ensure accurate threat detection and minimize false positives.

4.4.12. Vulnerability Management

a) Regular vulnerability assessments and scanning must be conducted to identify and remediate security weaknesses in network infrastructure, including routers, switches, and servers.
b) Critical vulnerabilities must be prioritized and promptly addressed to mitigate the risk of exploitation by malicious actors.

4.4.13. Network Segmentation

a) Network segmentation must be implemented to isolate sensitive systems and data from less secure areas of the network, reducing the impact of security breaches and limiting lateral movement by attackers.
b) Segmentation controls must be enforced using VLANs, access control lists (ACLs), and other network segmentation techniques.

4.4.14. Secure Configuration Management

a) A set of secure configurations must be selected for all network appliances before they are used by the enterprise.
b) If configuration guidelines are not available for a particular technology, ICT must research appropriate security configurations before using the product to develop a configuration template for this technology.
c) Every operating system, application, and device deployed in the enterprise network must be appropriately configured and meet security requirements for their purposes.
d) All enterprise laptops and workstations must utilize a host-based firewall or port-filtering tool, with a default-deny rule.
e) Default accounts shipped with operating systems and software, such as root, administrator, and other pre-configured vendor accounts must be appropriately disabled or configured to prevent unauthorized access (e.g., unauthorized password change).
f) Network Operating systems must be configured to automatically update, unless
g) Every network appliance deployed in the enterprise must be appropriately configured and meet security requirements for their individual purpose.
h) Automatic session expirations must be configured for network appliances.

i) Default accounts shipped with network appliances, such as root, administrator, and other pre-configured vendor accounts must be appropriately disabled or configured to prevent inappropriate access (e.g., password change).
j) All ports, protocols, and services not required to support operations must be disabled where possible.
k) Domain Name System (DNS) filtering services must be used on all enterprise assets to block access to known malicious domains.
l) ICT EO must configure network appliances to have detailed audit logging enabled.
m) ICT EO must ensure that sufficient space is available to collect and maintain audit logs.
n) All network devices and other infrastructure must be configured to automatically update, unless an alternative approved patching process is used.
o) ICT EO must only use up-to-date network management protocols (e.g., Secure Shell (SSH)
p) Securely configured technologies must be monitored to ensure they remain in compliance with approved configurations.
q) All protocols and tools used to install, modify, or otherwise manage technology configurations must be approved by ICT EO.
r) Network traffic must be monitored in real time, and comprehensive logs must be maintained to record network activities, including user authentication, access attempts, and system changes.
s) Log files must be securely stored and regularly reviewed for signs of unauthorized access, suspicious behavior, or security policy violations.
t) Regular security awareness training must be provided to all network users to educate them about common threats, phishing attacks, and best practices for maintaining network security.

u) Users must be encouraged to report suspicious activities and security incidents promptly to the ICT EO security team.

# 5. Server Security

5.1. Overview

The servers housed within the FMOH Data Centers serve as critical components supporting a diverse array of services catering to both internal and external stakeholders. These servers play a

pivotal role in storing, processing, and disseminating sensitive information pertinent to FMOH operations. However, the nature of their functionality renders them susceptible to potential security threats originating from external sources.

5.2. Purpose

The purpose of this policy and guidelines is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on FMoH's internal network(s) or related technology resources via any means. This can include, but is not limited to, the following:

- Internet servers (FTP servers, Web servers, Mail servers, Proxy servers, etc.)
- Application servers
- Database servers
- File servers
- Third-party appliances that manage network resources

This policy also covers any server device outsourced, co-located, or hosted at external/third-party service providers.

5.3. Policy Statements

a) All internal servers deployed at FMOH must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs, and approved by the InfoSec team. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by ICT EO. The following items must be met:
b) Servers must be registered within the inventory management system. At a minimum, the following information is required to positively identify the point of contact:

    i. Server contact(s) and location, and a backup contact
    ii. Hardware and Operating System/Version

iii. Main functions and applications, if applicable

c) Information in the Ministry's inventory management system must be kept up to date.
d) Configuration changes for production servers must follow the appropriate change management procedures
e) For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

5.4. Guidelines

### 5.4.1. Configuration Requirements

a) Operating System configuration should be approved by the ICT team.
b) Services and applications that will not be used must be disabled where practical.
c) Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
d) The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
e) Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
f) Always use standard security principles of least required access to perform a function. Do not uses root when a non-privileged account will do.
g) If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
h) Servers should be physically located in an access-controlled, secured environment.
i) Servers are specifically prohibited from operating from uncontrolled or unsecured cubicle areas.

### 5.4.2. Monitoring

a) All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

b) Security-related events will be reported to ICT, who will review logs and report incidents to ICT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
c) Port-scan attacks
d) Evidence of unauthorized access to privileged accounts
e) Anomalous occurrences that are not related to specific applications on the host.

# 6. ICT Security Incident Management

## 6.1. Overview

ICT Security Incident management is the ability to react to FMOH IT security incidents in a controlled, pre-planned manner. A security incident is defined by the INSA's Cyber- Emergency Response team (Ethio-CERT) as a breach of an IT system's security policy in order to affect its integrity or availability through unauthorized access or attempted access to an IT system

An IT incident may result in sensitive information being exposed, which might compromise FMOH business delivery or the Data Protection Act. An incident might also cause harm or damage to individuals or organizations and result in operational disruption or reputational damage to the FMOH.

## 6.2. Purpose

The purpose of an ICT security incident management policy is to establish a structured framework for effectively managing and responding to security incidents related to information and communication technology within an organization.

## 6.3. Policy Statements

a) All employees should be responsible for promptly identifying and reporting any incidents they encounter or suspect.
b) The incident identification process should be clearly outlined, including the steps for reporting incidents, the individuals or teams responsible for receiving and escalating reports, and the channels through which incidents should be reported.

c) Incidents should be classified based on their severity, impact, and potential risks to the organization.
d) Classification criteria shall be defined to categorize incidents into different levels or categories, enabling prioritization of incident response and resource allocation.

6.4. Guidelines

### 6.4.1. Incident Reporting

a) Responsible team shall develop an "Information Security Incident Management Form" in order to report all security violations/incidents which establish a quick response mechanism to information security incidents.

b) All employees must immediately report all suspected security related events to the ICT Department.

The following information shall be supplied, but not be limited to:

Contact name and number of people reporting the incident. The type of information or equipment involved. Whether the loss of the information puts any person or other data at risk is the location of the incident. Inventory numbers of any equipment affected. Date and time the security incident occurred Location of data or equipment affected. Type and circumstances of the incident all information security incidents shall be recorded and allocated an incident number for tracking and future reference.

### 6.4.2. Incident Response

a) The process to respond to an incident shall be described in detail in an Incident Response Plan.
b) Each ICT EO shall have an IT Security Incident Response Plan.
c) The response to an incident shall be logged
d) Responsible team must generate reports on incidents on a monthly basis and consolidate into the ITC Service Report every quarter
e) The actions required to recover from the information security incident shall be under a formal control. Only identified and authorized employees shall have access to the affected systems

during the incident; and all of the remedial actions shall be documented in as much detail as possible.

### 6.4.3. Incident Analysis and Investigation

Incident analysis and investigation, which may include the following steps:

a) Initial Assessment: Gather basic information about the incident, such as the date, time, location, and suspected cause.
b) Data Collection: Secure and preserve relevant evidence, such as system logs, network traffic, and user activity.
c) Interviewing witnesses: Gather information from individuals who may have knowledge of the incident.
d) Root Cause Analysis: Identify the underlying factors that contributed to the incident.
e) Documentation: Document all findings and activities throughout the investigation process.

### 6.4.4. Learning from Incidents

**a)** ICT related incidents shall be collated and review the post incident information on a regular basis. Any changes to the process made as a result of the post incident review shall be formally noted.

b) After each incident, a lessons-learned exercise shall be conducted by ICT responsible team shall be analyzed; and the results shall be adequately documented. The followings shall be considered: Conducting post incident analysis in a timely manner to determine the damage/cost incurred, confirm the cause, motive of the attack and any potential mitigating actions. Performing an assessment of the involved systems to ensure that no additional user accounts have been created and user privileges have not been modified during incident response.

### 6.4.5. Documentation and Record-Keeping

a) All incidents should be promptly documented, including the date, time, and nature of the incident, individuals involved, and any immediate actions taken.

b) This documentation will be maintained in a secure and accessible manner, in compliance with relevant regulations and best practices.
c) The document must be Clear and comprehensive.
d) All employees should expect to adhere to this policy and actively contribute to the documentation and record-keeping process. Any concerns or observations related to incident management should be promptly reported and documented according to our established procedures.

# 7. Internet Usage

## 7.1. Overview

Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:- Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet.

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Access to the Internet will be provided to users to support the Ministry's business activities and only on an as-needed basis to perform their jobs and professional roles.

## 7.2. Purpose

The purpose of this policy is to define the appropriate uses of the Internet by MOH employees and affiliates.

## 7.3. Policy statements

- Access to the Internet will be provided to users to support business activities and only to perform their jobs and professional roles.
- ICT EO shall have the responsibility to guarantee Internet access through proxy server (proxy.moh.gov.et).
- ICT EO has the responsibility to deal with ISP (Ethio telecom) for the appropriate band width and service availability of the Internet.

7.4. Guidelines

### 7.4.1 Allowed Internet Services

- ICT EO reserves the right to add or delete services as business needs change or conditions warrant.
- All other services other than the ministry business will be considered unauthorized access to/from the Internet and will not be allowed.
- Capabilities for the following standard Internet services will be provided to users as needed:
  - ❖ E-mail - Send/receive E-mail messages to/from the Internet through MoH's email system.( example Microsoft outlook)
  - ❖ Navigation - WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP or HTTPs) browser tool. Access to/from the Internet will be limited based on its importance and other constraints.
  - ❖ File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.
  - ❖ Telnet -- Standard Internet protocol for terminal emulation. Strong Authentication is required for Internet initiated contacts into the company.

### 7.4.2. Prohibited Internet Activities

The following uses of the Internet are strictly prohibited. This list is not all-inclusive but is intended to convey the usage that is potentially harmful to FMoH and ICT EO has to filter/control through its security control mechanism**:**

- Any interaction with Usenet groups, newsgroups, or other topic-based forums on the Internet, or with any Web sites providing material that:
  - ❖ Contributes to a hostile work environment
  - ❖ Can be construed as sexual harassment
  - ❖ Diminishes network performance (streaming media content, online games, Flash-intensive content, and so on)

- ❖ Promotes illegal activities of any kind
- ❖ Links to any unsuitable, questionable, or illegal material
- ❖ Provides "chat room" services that allow, provide, condone, or support online conversations or message threads that may be construed as generally offensive or defamatory, or that deride any group based on race, gender, religion, military status, creed, or ethnicity, or in any way contribute to a hostile work environment.

- Any interaction with sites or downloading materials that can.
  - ❖ Cause network problems
  - ❖ Compromise network security
  - ❖ Have a negative impact on the use or performance of the client computer
  - ❖ Transferring by email, Webmail, file transfer protocol (FTP), or by other non-secure electronic means, any materials expressly owned by FMOH (and implicitly confidential) such as financial, personnel data to any individual, group, computer, server, or any other entity outside of the FMOH network.

#### 7.4.3. Web access Exemption

ICT EO may guarantee Web Site Exemption for a limited duration or to a limited scope of employees based on the nature of the site and suitable justification for the exemption.

NOTE: No exemption under any circumstances will be granted for Web sites in the following categories:

- ❖ Pornography
- ❖ Mature content
- ❖ Sites dedicated to the promotion of hatred or violence
- ❖ Terrorist act

# 8. Security Surveillance System

8.1. Overview

The Security Surveillance System Policy outlines the guidelines and procedures for the deployment, management, and use of surveillance systems within the Ministry's ICT infrastructure.

8.2. Purpose

The primary purpose of the policy is to ensure the effective and ethical use of surveillance systems to enhance security, safety, and operational efficiency within the organization.

8.3. Policy Statements

a) Before deployment, a comprehensive assessment of surveillance needs and objectives shall be conducted to determine the optimal placement and coverage areas for cameras and equipment.
b) A site survey shall be conducted to identify key areas requiring surveillance coverage, taking into account factors such as lighting conditions, obstructions, and potential blind spots.
c) The cameras shall be mounted at an appropriate height and angle to capture facial features and activities effectively, avoiding extreme angles or heights that may compromise image quality or coverage.
d) The ICT and Security Office must ensure surveillance coverage of vulnerable areas prone to security threats or unauthorized access, including parking lots, loading docks, storage facilities, and perimeter fences.

8.4. Guidelines

### 8.4.1. Access Control and Authentication

Access controls and authentication mechanisms shall be implemented to restrict access to surveillance system controls and recorded footage, ensuring that only authorized personnel can view or manipulate surveillance data.

### 8.4.2. Data Retention and Storage

a) ICT shall develop a comprehensive retention policy outlining the procedures for storing surveillance data, including the duration for which data will be retained based on legal requirements, regulatory obligations, and organizational needs.
b) ICT shall ensure that the retention policy aligns with applicable laws, regulations, and industry standards governing the storage and retention of surveillance data, including data protection laws, privacy regulations, and industry-specific guidelines.
c) ICT shall classify surveillance data based on sensitivity and importance to the organization, distinguishing between different types of data such as live feeds, recorded footage, and metadata.
d) ICT shall implement encryption measures to protect stored surveillance data from unauthorized access or tampering, ensuring that data is encrypted both at rest and in transit to safeguard sensitive information.
e) ICT shall establish access restrictions and controls to limit access to surveillance data to authorized personnel only, utilizing role-based access controls (RBAC), user authentication mechanisms.
f) ICT shall deploy secure storage infrastructure capable of accommodating the volume and diversity of surveillance data, including on-premises servers, cloud storage solutions, or hybrid storage environments, ensuring redundancy and scalability.
g) ICT shall define specific retention periods for different types of surveillance data based on their relevance, legal requirements, and operational needs, ensuring that data is retained for an appropriate duration to support investigative, audit, or regulatory purposes.

### 8.4.3. Monitoring and Review

a) Regular monitoring and review of surveillance footage shall be conducted to proactively identify security incidents, suspicious activities, or policy violations, enabling prompt intervention and corrective actions as necessary.

### 8.4.4. Incident Response

a) ICT and Security Office shall establish protocols for responding to security incidents detected through surveillance systems, including predefined notification procedures, thorough investigation processes, and timely implementation of corrective measures to mitigate risks and prevent recurrence.

### 8.4.5. Privacy Protection

a) Measures shall be implemented to protect the privacy rights of individuals captured by surveillance cameras, including employee awareness initiatives, prominent signage in monitored areas, and practices such as data anonymization to minimize the risk of unauthorized disclosure or misuse of personal information.

### 8.4.6. Training and Awareness

a) The provision of comprehensive training and awareness programs shall be ensured for employees involved in surveillance system operations, equipping them with the necessary knowledge and skills to use the technology responsibly and in compliance with policy guidelines.

### 8.4.7. Enforcement

a) The Ministry shall develop procedures for enforcing compliance with the Surveillance System Policy, conducting regular audits and inspections, and addressing non-compliance issues through corrective actions and disciplinary measures.

### 8.4.8. Review and Revision

a) The policy shall be reviewed regularly and revision of the policy to incorporate changes in technology, regulations, and organizational requirements to ensure its continued effectiveness and relevance.

# 9. IT Auditing

9.1. Overview

This policy establishes the framework for conducting independent and objective audits of the organization's Information Technology (IT) systems and controls. The primary objective of IT audits is to assess the effectiveness of IT controls in safeguarding the organization's assets, ensuring data integrity, infrastructure and maintaining system reliability.

9.2. Purpose

The purpose of the IT Hardware and Software Audit Policy is to establish a structured framework for conducting audits of IT hardware and software assets within the organization.

9.3. Policy statements

- All information resources that create collect, store, and/or process confidential information must be audited on a regular basis, according to a documented schedule.
- The scope and conduct of information resource audits must be done in accordance with documented standards and/or procedures.
- Audit summary reports must be created for each system security audit conducted, and the reports must be provided to management at the conclusion of the audit.

9.4. Guidelines

### 9.4.1. IT Hardware and Software Audit

IT audits should be conducted in accordance with generally accepted auditing plan. The specific audit methodology used will vary depending on the type of audit being conducted.

a) Conduct regular and periodic audits based on a predefined schedule or trigger events such as system upgrades, acquisitions, or organizational changes.
b) Maintain accurate and up-to-date records of IT hardware and software assets, including purchase dates, warranties, serial numbers, and license agreements.

c) Ensure that audit procedures are conducted in a non-disruptive manner to minimize impact on ongoing operations and productivity.
d) Use automated tools and software solutions to streamline audit processes, enhance accuracy, and improve efficiency.
e) Collaborate with procurement, finance, and legal departments to verify compliance with licensing agreements, vendor contracts, and procurement policies.
f) Engage with third-party auditors or consultants as needed to supplement internal audit capabilities and ensure impartiality and objectivity.
g) Continuously evaluate and enhance audit processes, methodologies, and tools to adapt to evolving
h) Document audit findings, observations, and recommendations in a clear and concise manner for management review and decision-making.
i) Prioritize audit findings based on risk severity, potential impact, and urgency for remediation and resolution.
j) All employees are responsible for complying with this policy and for cooperating with network auditors during the audit process.
k) Simulating real-world attacks to assess system defenses and identify exploitable weaknesses.
l) Security incident and event management (SIEM): Correlating and analyzing security events from various sources for comprehensive insights.
m) The policy should be aligned with the organization's overall IT strategy and risk management framework.
n) The policy should be communicated to all employees.

### 9.4.2. External audit

a) Describe the policies and process for appointing the external auditors and the timeline of their tenure

b) Explain how the scope of the audit is determined and any specific areas of focus which the board/audit committee/shareholders have requested.

c) Explain the policy for the provision, by the external auditor, of non-audit services

d) Explain how the audit committee plans to monitor audit quality

### 9.4.3. Internal audit

- Describe the company's internal audit and assurance processes including to what extent management conclusions and judgments in the annual report and accounts are challenged and verified internally.
- To the extent that any items of the reporting matters noted above are subject to internal assurance, explain how the company is proposing to strengthen its internal audit and assurance capabilities to undertake this work.
- To enable the Internal Audit Division to accomplish its objectives, the following guidelines should be observed:
- internal auditors should receive the full support and cooperation of all levels of Institute management;
- internal auditors should be allowed access to all activities, records, personnel and any other material or information necessary to the proper performance of their duties;
- internal auditors should be notified promptly of any known or suspected activities of an illegal or unethical nature or any activities which appear to represent a conflict of interest;
- internal auditors should be informed on a timely basis of proposals for new or modified EDP systems, procedures, operations and programs;
- internal auditors should have no operational authority or responsibility for the activities which they audit; and,
- internal auditing should be conducted in accordance with an annual audit plan
- internal auditors should receive the full support and cooperation of all levels of Institute management;
- internal auditors should be allowed access to all activities, records, personnel and any other material or information necessary to the proper performance of their duties;
- internal auditors should be notified promptly of any known or suspected activities of an illegal or unethical nature or any activities which appear to represent a conflict of interest;

- internal auditors should be informed on a timely basis of proposals for new or modified EDP systems, procedures, operations and programs;
- internal auditors should have no operational authority or responsibility for the activities which they audit; and,
- internal auditing should be conducted in accordance with an annual audit plan

- Conduct regular and periodic audits based on a predefined schedule or trigger events such as system upgrades, acquisitions, or organizational changes.
- Maintain accurate and up-to-date records of IT hardware and software assets, including purchase dates, warranties, serial numbers, and license agreements.
- Ensure that audit procedures are conducted in a non-disruptive manner to minimize impact on ongoing operations and productivity.
- Use automated tools and software solutions to streamline audit processes, enhance accuracy, and improve efficiency.
- Collaborate with procurement, finance, and legal departments to verify compliance with licensing agreements, vendor contracts, and procurement policies.
- Engage with third-party auditors or consultants as needed to supplement internal audit capabilities and ensure impartiality and objectivity.
- Continuously evaluate and enhance audit processes, methodologies, and tools to adapt to evolving
- Document audit findings, observations, and recommendations in a clear and concise manner for management review and decision-making.
- Prioritize audit findings based on risk severity, potential impact, and urgency for remediation and resolution.
- All employees are responsible for complying with this policy and for cooperating with network auditors during the audit process.
- Simulating real-world attacks to assess system defenses and identify exploitable weaknesses.
- Security incident and event management (SIEM): Correlating and analyzing security events from various sources for comprehensive insights.

- The policy should be aligned with the organization's overall IT strategy and risk management framework.
- The policy should be communicated to all employees.

# 10. Email Security

## 10.1. Overview

MOH email security policies are important to encourage positive and productive communication while also protecting the organization from liability, data loss, interruption, reputation, and more. Therefore, an email policy will help ensure that employees are aware of their responsibilities when using email. Corporate email usage policy helps employees use their corporate email addresses appropriately. Email is essential to our everyday jobs. We want to ensure that our employees understand the limitations of using their corporate email accounts. The goal is to protect our confidential data from breaches and safeguard our reputation and technological property.

## 10.2. Purpose

The Purpose of this policy is to help the Organization reduce the risk of an email-related security incident, foster good communications both internal and external to the Organization, and provide for consistent and professional application of the organization email principles

## 10.3. Policy Statement

- MOH ICT EO shall implement a mail and collaboration system.
- All employees of MOH and consultants working for MOH are eligible to use the email system.

- All official business communications should be done using MOH's email address account.
- Users of MOH's IT facilities must take all reasonable steps to prevent the receipt and transmission by email of malicious software e.g. computer viruses.
- MOH ICT EO will maintain appropriate monitoring arrangements in relation to all Internet, email and related services and facilities that it provides, and will apply these monitoring arrangements to all users.

10.4. Guidelines

**10.4.1. Unacceptable Email Usage**

a) Sending any information that is illegal under applicable laws;
b) Accessing another user's email account without the knowledge or permission of that user, which should only occur in extreme circumstances, the approval of Organization executives in the case of an investigation, or when such access constitutes a function of the employee's normal job responsibilities;
c) Sending any emails that could cause embarrassment, reputation damage, or harm to the MOH;
d) Spreading messages with insulting, biased, racist, harassing, annoying, threatening, or otherwise inappropriate messages or media;
e) Sending emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally provocative or contain information that is not appropriate for a professional working environment.
f) Attempt to impersonate someone else or forge an email header;
g) Intentionally spreading viruses, sending spam messages, chain letters, and solicitations;
h) carrying on non-corporate business, sending unauthorized marketing or solicitation emails;
i) Signing up for websites and services that are illegal, untrustworthy, dishonest, or suspicious;
j) Using a corporate email address to send confidential data without authorization;
k) Setting up a corporate email account to automatically forward messages to an Internet Mail account;

l) Using a corporate email account for side business communications;
m) Forging or attempting to forge email messages, as well as concealing or attempting to conceal your identity when sending mail, are all prohibited.

### 10.4.2. Appropriate Use of Corporate Email

Employees shall to use their email to:

a) Contact current or prospective customers and partners;
b) Give their email address to people they meet at conferences, career fairs, or other corporate events for business purposes;
c) Sign up for newsletters, platforms, and other online services that will assist them in their jobs or professional development.

### 10.4.3. Email Security

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality, and security of our equipment. Employees should:

a) Select strong passwords with at least eight characters (capital and lower-case letters, symbols, and numbers) without using personal information (e.g., birthdays) and default passwords;
b) Remembering passwords rather than writing them down and keeping them confidential;
c) Employees' email passwords should be changed every three months;
d) Avoid opening attachments and clicking on links when content is not adequately explained;
e) Verify that unknown senders' email addresses and names are genuine;
f) If an employee is unsure whether an email they received is secure, they can consult with Cyber Security Specialists.

### 10.4.4. Personal Use

a) Users are required to use a non-corporate-provided (personal) email account for all non-business communications. The corporate email system is for corporate communications.

b) Users must follow applicable policies regarding the access of non-corporate provided accounts from the corporate network.
c) Employees are allowed to use their corporate email for personal reasons. For example, employees shall use their corporate email to:
    i. Sign up for classes or meetups;
    ii. Send emails to friends and family as long as they are not spam or contain sensitive information;
    iii. Download eBooks, guides, and other content for their personal use as long as it is safe and appropriate.

### 10.4.5. Sending Emails

a) Emails sent from corporate email accounts must be addressed and sent carefully. Users should keep in mind that once email is sent outside of the corporate network, the corporate loses control.
b) Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled, using the reply all function, or using distribution lists, in order to avoid inadvertent information disclosure to an unintended recipient.

### 10.4.6. Email Signatures and Auto-Responders

a) An email signature (contact information appended to the bottom of each outgoing email) is recommended for emails sent from the corporate email system. At a minimum, the signature should include the user's:
b) The title, company name, phone number(s), and URL for the corporate website are all required.
c) Email signatures shall not include personal messages (political, humorous, etc.). The IT department is able to assist with email signature setup if necessary.
d) MOH recommends the use of an auto-responder if the user shall be out of the office for an entire business day or more.
e) The auto-response should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required.
f) Employees shall also include professional images, MOH logos, and work-related videos and links in email signatures.

### 10.4.7. External Email Accounts and Instant Messaging

a) The use of external email accounts such as web mail is not prohibited, but for security reasons, email users are expected not to use these external email accounts to send, receive, and store any official data.
b) Instant messaging applications such as MSN, Yahoo Messenger, etc. are prone to malicious code. More precisely, these applications can be used as entry points for viruses and worms into the MOH computer network.

### 10.4.8. Prevention of Malicious Software

Emails are subjected to huge amounts of malicious software, including viruses, computer worms, and spyware. As a result, MOH must implement technical measures to ensure that malicious computer software is prevented from entering the network and infecting computer systems. The following will govern incoming and outgoing malicious or potentially harmful attachments:

a) All virus-infected email is blocked by default;
b) All attachments that cannot be scanned for viruses will also be blocked;
c) Typical virus hoaxes will be blocked;
d) All executable files and documents containing embedded executable will be restricted;
e) All unknown/unrecognizable attachments will be blocked;

Users should:

I. Never open unsolicited email attachments;
II. Never open email attachments from unknown sources;
III. Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially formatted emails can hide a malicious URL.

### 10.4.9. Access to another Employees Email

a) No employee, except authorized security personnel, is allowed to access another employee's emails or mailbox.

b) If an email user requires another employee (the delegate) to access his or her emails, then he or she must complete the Email Authorization Form and submit it to the IT support Office.

c) To view the contents of employees' electronic communications and email activity or history in the course of problem resolution, system maintenance, and operational duties.

### 10.4.10. Mass Email

**a)** Mass emails shall be useful when communicating with the company's employees or customer base) and are allowed as the situation dictates.

b) The sending of spam, on the other hand, shall be strictly prohibited.

c) It is the MOH intention to comply with applicable laws governing the sending of mass emails. For this reason, as well as in order to be consistent with good business practices, the corporation requires that email sent to more than twenty (20) recipients external to the MOH have the following characteristics:

d) The email must contain instructions on how to unsubscribe from receiving future emails (a simple reply to this message with UNSUBSCRIBE in the subject line will do). Unsubscribe requests must be honored immediately. B. The email must contain a subject line relevant to the content. C. The email must contain contact information for the sender. D. The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.

e) Emails sent to MOH employees, existing customers, or people who must inquire about MOH's services are exempt from the above requirements.

### 10.4.11. Classified Data

a) Sensitive data should be sent via an encrypted attachment and not in plain text within an email.

b) Passwords used to access email accounts must be kept confidential and used in accordance with the Password Policy.

c) The MOH must further secure email with certificates, two-factor authentication, or another security mechanism.

d) Unauthorized emailing of MOH data, confidential or otherwise, to external email accounts for saving this data external to MOH systems shall be prohibited.
e) If a user needs access to information from external systems (such as from home or while traveling), that user should notify his or her supervisor rather than emailing the data to a personal account or otherwise removing it from MOH systems.
f) The MOH shall employ data loss prevention techniques to protect against the leakage of confidential data.

### 10.4.12 .Filtering

a) The MOH shall filter email at the Internet gateway and/or the mail server in an attempt to filter out spam, viruses, or other messages that may be deemed i) contrary to this policy, or ii) a potential risk to the MOH IT security.
b) When opening emails, the user shall be aware of this policy and use common sense.
c) Many email and/or anti-malware programs shall identify and quarantine emails that they deem suspicious.
d) This functionality may or shall not be used at the decision of the IT Security Manager, or their designee.
e) Users must understand that the MOH has little control over the contents of inbound email and that this email may contain material that the user finds offensive.

### 10.4.13. Account Activation

a) MOH emails accounts shall be set up for each user determined to have a business need to send and receive email.
b) Accounts shall be set up at the time a new hire starts with the corporate, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email.

### 10.4.14. Account Termination

a) When a user leaves the MOH, or his or her email access is officially terminated for another reason, the MOH Shall disable the user's access to the account by password change, disabling the account, or another method.
b) The MOH is under no obligation to block the account from receiving email and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the Organization no longer employs the user.

# 11. Operating System and Application Software

11.1. Overview

An Operating System (OS) and Application Software Policy and guidelines serve as a comprehensive framework for managing and securing the software environment within MOH. This policy outlines guidelines, procedures, and best practices to ensure the effective deployment, maintenance, and security of operating systems and application software. The primary objective is to establish a secure and standardized computing environment that aligns with MOH goals, industry regulations, and compliance requirement

11.2. Purpose

The primary purpose of this policy is to establish a resilient, secure, and standardized computing environment that harmonizes with MOH objectives, industry regulations, and compliance mandates.

11.3. Policy Statements

- MOH ICT EO shall regularly standardize operating systems and any end user application software to be used in the Ministry. All procured software should be licensed and genuine.

11.4. Guidelines

a) All proprietary software used on personal devices and servers must be properly licensed.
b) Users are not permitted to install any unauthorized software onto computers, servers and on any IT equipment connected to the FMOH network.

c) Installation of FMOH licensed software on computers not owned by the organization is strictly prohibited
d) The ICT EO shall obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.
e) Software license registers shall be maintained by the ICT EO to ensure compliance with legislation.
f) Requests for procurement , modifications, enhancements and upgrades of existing software applications should be discussed and approved by ICT EO
g) In the course of software updates/changes there should be a mechanism by which the version control and an audit trail for all software changes requests are traced.
h) ICT EO implements licensed software regularly assessing the requirement for the new software within the context of FMOH mission, strategy and current technology needs.
i) The ICTEO shall provide recommendations regarding the preferred type and version of the operating system and application software to be installed on user devices and servers.
j) Users are not allowed to install operating systems on FMOH procured devices.
k) Except for software set for automatic updates, ICT EO staff should perform or configure all software updates to ensure compatibility with systems and applications
l) Installation of the latest version or patch/update should be implemented by ICT EO after extensive and successful testing. A roll back strategy should be in place before updates/upgrades are implemented.
m) The updating of operational software, applications, and program libraries should only be performed by ICT EO
n) ICT EO shall provide software training for users on basic application software.
o) ICT EO shall keep software disks, manuals and Software license inventory in a safe storage area.
p) All software requirements ought to go through ICT EO.

# 12. User Management

## 12.1 Overview

This policy document outlines the guidelines that users, administrators, technical personnel, and third parties must adhere to when accessing the ministry's ICT infrastructures

## 12.2. Purpose

The purpose of this policy is to provide a standardized framework for the systematic creation, administration, utilization, and termination of accounts that act as gateways to the ministry's ICT resources. By doing so, this policy aims to improve the efficiency, security, and accountability of ICT usage within the ministry.

## 12.3. Policy Statements:

## 12.4. Guidelines

### 12.4.1. Termination of employees

**Termination of Employees:**

- Work processes shall notify ICT of termination of employees in writing.
- Upon transfer/return of equipment, user data should be completely removed from the PC using appropriate tools/methods.
- Data belonging to MOH shall be transferred to the appropriate person.
- MOH ICTEO shall disable and then delete user accounts belonging to terminated/resigned users.
- Data stored on equipment belonging to terminated users shall be removed in an appropriate manner.
- On resignation or termination of employment, users should handover all the equipment and credentials to the relevant bodies. This should be considered as part of the

clearance procedure.

**12.4.2. MOH User:-**

- ❑ Should not use MOH ICT systems for personal business.
- ❑ Should not install any Software and Hardware on their PC without consulting MOH ICT EO
  - Are not allowed to add or modify network connections and any configurations.
- ❑ Should not use external speaker by any means
- ❑ Not affect the identification codes of their machine by any means
- ❑ Use their identity to get access to MOH's ICT resources
- ❑ Keep their identity properly; change their passwords regularly
- ❑ Not pass their identity to second party including colleague
  - No personal data files may be stored on the MOH computer system or on individual workstations.
- ❑ Perform their operations through proper ICT equipment
- ❑ Place their equipment in an appropriate position
- ❑ Keep their equipment clean
- ❑ Never put and/or use food or beverages near PCs
- ❑ Keep all accessories, including driver and recovery CDs in a safe place
  - Will be given access to appropriate network printers. In some limited cases, users may be given local printers if deemed necessary by MOH ICT EO.
  - Will be given as much as possible one Desktop computer or Laptop computer not both. In some limited cases, a user may be given both if deemed necessary by MOH ICT EO and Departments.
  - Shall not in any way affect the proper utilization of shared resources, such as printers.
  - will have the responsibility for the acceptable use of the hardware

- Shall under no circumstances remove/replace parts of hardware.
- Users are responsible for handling the IT equipment (PC, printers,Laptop,Tablet etc.) properly.

# 13. Password

## 13.1. Overview

Passwords play an essential role serving as a key safeguard for security of user accounts and sensitive information within the ministry's ICT infrastructure. This policy establishes standards for creating, managing, and securing passwords, aiming to mitigate the risk of unauthorized access, data breaches, and cyber threats.

## 13.2. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, protection of those passwords, and the frequency of change.

## 13.3. Policy statements

- Credential accounts to access any system should only exist for authorized personnel.
- Every employee must be uniquely identified by a name or number and belong to a group.
- Every user account created initially will have a default password given by the system administrator
- Users should change their provided password after first logon to the system.
- Users should not disclose or share their password to others that could be used to gain access to their own or any other account and they should not use another person's credentials.
- User passwords will not be changed by system administrators, except on request from the owner of the account.

- Each user should have only one account on a system (domain based)
- If guest accounts are used, their privileges should be very limited to what they entitled to
- Every ICT equipment in the organization should lock the screen after 15 minutes idle time with password protection
- Administrator accounts should be protected very carefully and shouldn't be shared. Only authorized administrators shall have full privilege for administrator account.

13.4. Guidelines

Passwords for the ministry's IT infrastructures and systems access must be implemented according to the following guidelines:

a) All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
b) All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 120 days.
c) Passwords must NOT be inserted into email messages or other forms of electronic communication.
d) Passwords must not be written down and stored anywhere in any office.
e) Passwords must not be shared with anyone (including supervisors, co-workers, administrative assistants or secretaries,).
f) The same password must not be used for multiple accounts
g) Users must not hint at the format of a password.
h) If the security of an account is in question or suspected to have been compromised, the password must be changed immediately.
i) In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report to ICT EO.
j) Users must not circumvent password entry with an auto logon, application remembering, embedded scripts, or hard coded passwords in client

software. Exceptions May be made for specific applications like automated backup processes with the approval of the ICT EO.

k) Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with MoH
l) Default passwords on systems must be changed after installation.
m) Enforcement of strong passwords will be automated if this feature is available in an application.
    - Minimum password length should be 8 characters.
    - Minimum complexity: passwords should use a combination of upper case, lower case, numbers and special characters, no dictionary words.
n) Password resets shall be requested only by the owner of the account except in exceptional cases as may be determined by the ICT EO.
o) Applications must implement standard encryption when storing passwords.

# 14. Hardware Procurement

## 14.1. Overview

With the continuous growth in the number of employees within the ministry and technological advancement, the demand for procurement of ICT equipment and systems is becoming increasingly significant. It is evident that acquiring and implementing ICT hardware entails substantial investment and due attention. Thus, the implementation of policy guidelines for the acquisition, deployment, and utilization of hardware in the Ministry of Health (MOH) is crucial to effectively manage these processes and ensure their proper adherence.

14.2. Purpose

This ICT hardware policy establishes guidelines that govern the acquisition, usage, maintenance and disposal of hardware resources within the Ministry of Health. It also aims to ensure, secure and cost effective hardware resources while aligning with the MOH goals and best practices.

14.3. Policy Statements

- To take advantage of ICT tools in the most cost-effective manner possible, MOH will standardize a series of hardware and software products that integrate easily with MOH IT infrastructure. ICT EO will maintain and make available an up-to-date list of supported hardware and software together with technical specification.
- While the acquisition of standard products is encouraged, some core/support processes have a need for special equipment or software which may not be included in the list of supported products. ICT EO will consult with them to select the most appropriate equipment and to work out an agreement for continued support.
- All procured software should be licensed, genuine and as much as possible shall meet the standard set by ICT EO.
- Core/Support processes are not allowed to procure or receive any ICT resources without the knowledge of the ICT EO.

14.4. Guidelines

**14.4.1. Hardware Procurement and Acquisition**

a) The procurement and acquisition of ICT hardware resources should be made in accordance with the 'ICT hardware and software procurement policy' of the ministry.

**14.4.2. Hardware/IT Equipment Usage**

To ensure efficient hardware provision and responsible usage within the ministry, the following measures should be implemented:

a) **Hardware Provision:** Eligible users should be provided with appropriate hardware/ICT equipment based on the business needs and requirements.

b) **Hardware Upgrade Proposal:** The ICT EO is responsible for assessing and upgrading hardware that does not meet the minimum requirements on a regular basis.
c) **Hardware Inventory Management**: The ICT EO should maintain an up-to-date hardware inventory, including information such as equipment type, owner, location, and other relevant details.
d) **Printer Access**: Users will be granted access to appropriate network printers. In certain limited cases, users may be provided with local printers if deemed necessary by their department and the ICT EO.
e) **Computer Provision**: Depending on the nature and responsibilities of the user, an employee will be provided with either a desktop computer or a laptop computer to the best extent possible. In some limited cases, a user may be provided with both if deemed necessary by the ICT EO and their department.
f) **Proper Utilization of Shared Resources:** Users must not interfere with the proper utilization of shared resources, such as printers, and should follow established protocols and guidelines.
g) **Permission for External Hardware**: No outside hardware equipment connected to the MOH network without the explicit permission of the ICT EO. If available wifi access will be provided
h) **Responsibility for Hardware Use**: The owner of the hardware is responsible for ensuring the acceptable use of the equipment.
i) **Hardware Integrity**: Users must not disassemble, remove, or replace parts of hardware that belong to the ministry.
j) **Inspection:** Any hardware whether it is obtained via procurement or through donations should pass through proper inspections by ICT EO before being put into use.

#### 14.4.3. Return of Equipment

To ensure the proper management of Ministry of Health -provided ICT equipment, the following guidelines are in place:

a) **Return of Equipment:** When an employee's employment or contract ends, it is mandatory for them to promptly return all Ministry of Health provided ICT hardware. This includes laptops, desktops, mobile devices, and any other equipment assigned to them.
b) **Data Removal and Preparation**: Upon receiving the returned hardware, the ICT EO will conduct thorough checks to ensure the removal of all sensitive data. Additionally, the hardware will be prepared for reuse or disposal as deemed appropriate by the ICT EO.

c) **Deactivation of User Account**: It is essential to deactivate the employee's user account associated with returned equipment as soon as the equipment is returned.

#### 14.4.4. Hardware Repairs and Maintenance

To ensure the smooth operation of ICT-related hardware, the following measures have been put in place:

a) **Repairs, Maintenance, and Upgrades**: All repairs, maintenance, and upgrades of ICT-related hardware shall be carried out by the ICT EO.
b) **Outsourcing with Supervision**: In cases where outsourcing of hardware maintenance is necessary, it should be done under the supervision and approval of the ICT EO.
c) **Preventive Maintenance**: To proactively address potential issues, preventive maintenance should be conducted by the ICT EO every six months for each hardware equipment

# 15. Network

### 15.1. Overview

The Ministry of Health (MOH) provides data center and network infrastructure services to its offices and employees, including wired and wireless connections. The purpose of this policy is to establish ownership of the MOH network infrastructure and outline the responsibilities of MOH staff and other users in protecting and securing these resources.

### 15.2. Purpose

This policy acts as a set of instructions for network and system administrators to effectively and appropriately manage the network infrastructure of the Ministry of Health (MOH).

15.3. Policy Statements

- ICT EO should avail appropriate network infrastructure, network services & resource access to every user in the MOH.
- ICT EO shall implement proper network security and document it so that the authorized users can access it.
- MOH will make available the Internet access to all in the compound for users to support their tasks and solely to perform their jobs and professional roles.

15.4. Guidelines

a) ICT EO should design, implement and maintain its network architecture with the appropriate level of administrative and technical security controls.
b) The network architecture should be designed and implemented by the appropriate defense mechanism for the physical access and remote access control from unauthorized users.
c) Compliance with national and international standards should be ensured when designing network and data center technologies for the ministry.
d) ICT EO should avail appropriate network services & resource access to MOH users to solely perform their jobs and professional roles.
e) ICT EO shall implement proper network security and document it so that the authorized users can access it.
f) Internet access shall be through dedicated appropriate technology
g) ICT EO is primarily responsible for overseeing the operations of the Network Infrastructure.
h) Users are expected to comply with MOH IT policies and procedures
i) ICT EO must establish a process for changing the configuration guides, which includes review and approval by authorized personnel.

j) System administrators are responsible for maintaining active and current antivirus protection on all applicable components of the MOH ICT equipment they oversee.
k) Unauthorized access, tampering, and interference with the MOH Network Infrastructure are strictly prohibited.
l) ICT EO is authorized to monitor the Network Infrastructure and take proactive measures, including scanning, to maintain the operation and security of the Network Infrastructure.
m) ICT EO reserves the right to revoke privileges to use or access any or all components of the MOH Network Infrastructure for non-compliance with this and other applicable information security policies.
n) Both newly purchased Access Points and existing ones must conform to the recommended specifications outlined by the ICT EO.

o) Proactive monitoring of wireless networks shall be conducted by ICT EO on a regular basis and any unauthorized Access Point will be removed from the network.
p) The installation and maintenance of all wireless connections and any request for installation of new Access Points must be directed through the ICT EO.
q) Wireless access points should require user authentication at the access point before granting access to MOH network or Internet services.
r) ICT EO has the responsibility to deal with ISPs for the appropriate band width and service availability of the Internet.

# 16. Data Center

## 16.1. Overview

The data center policy plays a critical role in establishing the principles, guidelines, and procedures necessary for the effective management and security of data centers. This

policy encompasses regulating physical access through authentication and authorization processes, as well as formulating robust security measures for safeguarding the data center infrastructure.

### 16.2. Purpose

This Data Center Policy establishes guidelines and procedures for the secure, efficient, and reliable operation of the data center within MOH. The policy applies to all personnel, including employees, contractors, and third-party vendors, who have access to the data center facilities or are, involved in data center operations.

### 16.3. Policy Statements

- The data center should be designed and equipped according to the standard
- Access to the data center is restricted.
- Authorized personnel shall use access-control devices, such as card swipe access

### 16.4. Guidelines

a) Data center design, construction, operation and management should follow guidance of international standards
b) Access to the data center is restricted to authorized personnel.
c) When access to the data center is required, proper notification and justification needs to be provided.
d) Casual visits and/or tours of the data center are not allowed. In exceptional cases, however, approval of a tour or casual visit may be granted to visitors. Requests for such visits should be directed to and approved by the network ICT EO. Food and drinks are strictly prohibited inside the Data Center premises
e) All equipment within the data center should be labeled.
f) No hardware, software, furniture, shelving or other materials will be removed or added to the Data Center without prior approval of ICT EO
g) All equipment must be rack mountable. Exceptions must be approved by ICT EO
h) The Data center must be kept clean and dust-free at all times. All doors and windows shall be closed at all times.

i) The data center services must be available at all times, 24/7
j) Hazardous or combustible materials should not be stored in the data center.
k) Implement systems to maintain optimal temperature and humidity levels for equipment performance.
l) Approved server configuration guides must be established and maintained
m) All Servers must be registered within the ICT EO equipment management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact.
    - Server IP address and role assigned to
    - ardware and Operating System/Version.
    - Main functions and applications installed, if applicable.
    - Full documentation must be prepared about configuration and installation.

# 17. ICT Support

## 17.1. Overview

The ICT Support Policy serves as a framework to guide users in accessing and receiving support for information and communication technology (ICT) resources within the ministry. This policy outlines the procedures, expectations, and responsibilities associated with IT support services, aiming to ensure efficient issue resolution and the optimal use of technology resources.

## 17.2. Policy Statements

- Hardware and software items purchased by MOH will normally be installed and supported by ICT EO.
- Users should get ICT related support from ICT EO only;
- ICT EO will provide such support and advice on specific IT problems as is possible, but cannot provide full-time computer support across the whole range of the work processes' activities.

- ICT EO shall provide IT support to users with minimal possible response time
- Where IT staff are unable to provide specific support, ICT EO can solicit the service of third-parties for support on a need base
- Support may be limited by a lack of expertise, difficulty or inability to connect the equipment to the network, inability to obtain replacement parts, inability to obtain warranty service, or other causes reasonably beyond the control of ICT EO staff

17.3. Guidelines

## a) Service Desk Contact

**Service Desk Availability:** The IT support service desk is available during regular business hours to address user inquiries, technical issues, and service requests.

**Contact Channels:** To seek IT support, ministry of Health employees/users have the option to submit requests via the MOH Support Portal (helpdesk.moh.gov.et) or through email at support@moh.gov.et.

For urgent matters requiring immediate attention, report emergency issues promptly using the fastest available communication channel.

### b) Requesting IT Support

**Service Request Procedures:** Users are required to submit service requests through the designated channels. Requests should include detailed information about the issue, relevant error messages, the user's contact information and department.

**Prioritization:** IT support will prioritize service requests based on severity and impact on business operations. Urgent issues affecting critical functions will receive immediate attention.

### c). Remote Support

**Remote Assistance:** IT support may utilize remote assistance tools to diagnose and resolve issues. Users must grant permission for remote access, and the session will be conducted securely.

**User Responsibilities:** Users are responsible for providing accurate information, cooperating during remote assistance sessions, and following any instructions provided by the IT support team.

### d). On-Site Support

**On-Site Visits**

For issues that cannot be resolved remotely, IT support may schedule on-site visits. Users should ensure their availability and provide access to necessary resources during on-site visits.

**Appointment Scheduling**

Users are encouraged to schedule on-site support appointments in advance to minimize disruptions to their work.

### e). Hardware and Software Support

**Hardware Issues**

IT support will address hardware issues, including repairs and replacements, according to established procedures. Users should report hardware problems promptly.

**Software Support**

IT support will assist with software-related issues, including installations, updates, and troubleshooting. Users should not attempt to install or modify software without prior approval.

### f). SUPPORT FOR PERSONAL EQUIPMENT

- Support will not be granted for personally owned software and hardware problems on personally owned IT equipment.
- Support may be granted if the IT Service authorizes the use of personal equipment for MOH's purposes.

### g). Reporting Security Incidents

**Security Concerns**

Users must promptly report any suspected security incidents or breaches to the IT support team. This includes lost devices, unauthorized access, or suspicious activities.

# 18. IT Training and awareness creation

18.1 Overview

Information and Communication Technology (ICT) has become an essential part of our daily lives and plays a crucial role in the success of any organization. To ensure our staff are proficient and confident in using technology to their full potential, this ICT Training Policy outlines the organization's commitment to providing ongoing training and development opportunities.

18.2. Purpose

The aim of the training policy is to ensure that all employees are given the necessary help to develop the knowledge, skills and attitude that they require to carry out their jobs efficiently and be able to better protect MOH's IT resources from unauthorized intrusion or data compromise. This policy will help prevent the loss of data and organizational assets.

18.3. Policy Statements

- MOH commits itself to providing continuous training and development to improve the skills and competence of its entire workforce.
- MOH shall adopt PC literacy as a pre-requirement for employment.
- ICT EO shall assess MOH staff ICT related training gap and build the capacity of staff on a regular basis.

18.4. Guidelines

## Training Objectives

### 18.4.1. Skill Enhancement:

a) Provide training opportunities to enhance employees' ICT skills, ensuring proficiency in the use of relevant technologies and tools.

b) Facilitate continuous learning to keep employees abreast of emerging trends and advancements in the ICT field.
c) Provide induction on for new employees up on requisition of ICT equipment

#### 18.4.2. Security Awareness:

a) Integrate security-focused training modules to enhance awareness of ICT security risks and promote responsible technology use.
b) Equip employees with the knowledge and skills needed to identify and respond to potential security threats.

#### 18.4.3. Efficient System Utilization:

a) Promote the efficient use of ICT systems, applications, and tools to maximize productivity and streamline business processes.
b) Ensure that employees are well-versed in utilizing organization-approved software and technology resources.

### Training Programs

#### 18.4.4. Mandatory Training:

a) Identify essential ICT training programs that are mandatory for all employees based on their roles and responsibilities.
b) Specify the frequency and timelines for mandatory training sessions.

#### 18.4.5. Role-Specific Training:

a) Tailor training programs to address the specific ICT needs of different roles within the organization.
b) Ensure that employees receive training relevant to their job functions to enhance job performance.

#### 18.4.6. Customized Training Plans:

a) Develop customized training plans for teams or departments with unique ICT requirements.
b) Allow flexibility in training delivery methods to accommodate varying learning styles and preferences.

## Training Delivery

### 18.4.7. In-House and External Resources:

a) Utilize a combination of in-house expertise and external resources to deliver comprehensive and up-to-date ICT training.
b) Collaborate with external training providers when specialized knowledge is required.

### 18.4.8. E-Learning Platforms:

a) Implement e-learning platforms to provide on-demand training resources, allowing employees to learn at their own pace.
b) Track and monitor employee progress through e-learning modules.

## Evaluation and Feedback

### 18.4.9. Assessment and Certification:

a) Conduct assessments to evaluate the effectiveness of ICT training programs.
b) Issue certifications or recognition to employees who successfully complete training courses.

### 18.4.10. Feedback Mechanism:

a) Establish a feedback mechanism to gather input from employees regarding the quality and relevance of ICT training.
b) Use feedback to continuously improve training programs.

## Policy Compliance

### 18.4.11. Mandatory Participation:

a) Mandate employee participation in designated ICT training programs.
b) Specify consequences for non-compliance with mandatory training requirements.

# 19. MOH Electronic mail service

## 19.1. Overview

MOH has internal Electronic Mail Service that enables users to share information and exchange ideas, as a means of communication. This policy is designed to ensure the proper usage of MOH's Email service.

## 19.2. Purpose

The purpose of this Electronic Mail (email) policy is to establish compliance requirements for conducting for the ministry through email and the management practices that support email services.

## 19.3. Policy Statements

- MOH shall implement a mail and collaboration system.
- All employees of MOH and consultants working for MOH are eligible to use the email system.
- All official business communications should be done using MOH's email address account.
- Users of MOH's ICT facilities must take all reasonable steps to prevent the receipt and transmission by email of malicious software e.g. computer viruses.
- MOH ICT will maintain appropriate monitoring arrangements in relation to all Internet, email and related services and facilities that it provides, and will apply these monitoring arrangements to all users.
- When new employee is hired, the work process is responsible to request MOH ICT for e mail account.
- The email address of every employee will have the following structure:
    - *'first letter of employee '&'middleName'&'@moh.gov.et'*

E.g. Abebe Kebede email address will be: akebede@moh.gov.et

## 19.4. Guidelines

### 19.4.1. Account Request for Eligible Users

- When new employee is hired, the work process is responsible to request MOH ICT for email account.
- Work Processes may request e-mail accounts to ICT EO for guests who are in some way affiliated with MOH.
- ICT EO will grant the e-mail account based on the request by the work process.
- Work processes should notify the ICT EO when relationship of the account holder with MOH no longer exists.
- The email address of every employee will have the following structure:
    - *'first letter of employee '&'middleName'&'@moh.gov.et'*

      E.g. Abebe Kebede email address will be: akebede@mofed.gov.et

### 19.4.2. Disk Space Quota

- Email service users on the MOH network will get disk space on the mail server. Currently, this quota is set to 1GB with the possibility of applying for an increase in space if need be justified.
- If users do not read their mail often enough, their disk space may fill up, and mail sent after users have exceeded their quota will be bounced back to the sender with an error message.

### 19.4.3. Account Disabling and Deletion

Disable means that the account is still able to receive mail, but users will not be able to send message. During deletion, the user will be no long be able to use MOH mail account.

- To use the email service, a user must be currently an employee of MOH either in

permanent or contractual bases, a consultant or a guest. If they leave MOH, their account will be disabled or deleted.

- An account will be disabled or deleted when account audit is performed, when ICT believe that the user violet acceptable use of mail service.
- If users' account remains disabled for two months without being reactivated, then the next time an account audit is performed, it will be deleted and, hence, they will no longer be able to use e-mail service at MOH unless an account is created again.

# 20. Software Procurement

20.1. Overview

This policy establishes guidelines for the procurement of all computing and communication hardware and software in order to maximize MOH's investment in Information Technology (IT). The policy facilitates the selection of appropriate technology and made Tradeoffs between cost and quality of technology.

20.2. Policy Statements

- To take advantage of ICT tools in the most cost-effective manner possible, MOH will standardize a series of hardware and software products that integrate easily with MOH IT infrastructure. ICT EO will maintain and make available an up-to-date list of supported hardware and software together with technical specification.
- While the acquisition of standard products is encouraged, some core/support processes have a need for special equipment or software which may not be included in the list of supported products. ICT EO will consult with them to select the most appropriate equipment and to work out an agreement for continued support.
- All procured software should be licensed, genuine and as much as possible shall meet the standard set by ICT EO.
- Core/Support processes are not allowed to procure or receive any ICT resources without the knowledge of the ICT EO.

20.3. Guidelines

**ICT EO Should:**

- Be responsible for supporting the finance & procurement sub process by preparing the specification for minimum standard should be full filled procuring quality software.
- Propose the procurement of ICT equipment based on inventory result of equipment's regularly
- Decide on the appropriateness of request for purchase based on certain factors; not all procurement requests may be approved.
- Consider relevant parameters (inter-operability, latest technology, investment cost, availability, warranty, etc) to prepare suitable specification and revised it every three month.
- Perform technical evaluation of software procurement bids
- Respond to any technical complaints/suggestions that might be raised from suppliers.
- Make full Inspection of the purchased products up on delivery and Certify equipment's upon delivery
- Install and configure the equipment as per the MOH policy

- Consult the ICT EO for any technical assistance related to the procurement of any software.
- Before making any payment to suppliers, should get written approval for the confirmation of ICT EO whether they are up to the required specification

# 21. Software Development

21.1. Overview

This section of the IT policy describes the standardization guidelines & procedures for in-house

or third party software development as well as deployment and management.

### 21.2. Purpose

The purpose of software development Policy is to standardize software development for all enterprise-level centrally-managed mission critical web applications and web services through the use of industry leading practices.

### 21.3. Policy Statements

- ICT shall standardize software development tools for in-house as well as third-party software development based on the skills & knowledge of development staffs. Moreover, Priority shall be given to Open Source development tools.
- Software that is outsourced to the third party. This outsourcing environment shall build the capacity of the staff.
- ICT shall standardize in house software development.
- Software must be developed using the standard software development life cycle.
- ICT shall undertake regular system requirement study, develop software and provide training for users before the software is implemented and deployed.
- Software must be installed in ICT server and managed by system administrators.
- Work processes should provide full system information and assign relevant personnel to work with ICT's development team during requirement analysis.
- ICT has the responsibility to appoint project Manager
    - To achieve individual accountability for systems development activities
    - To co-ordinate ICT security activities associated with systems development
- System documentation and user manual should be part of the information system development process.
- ICT shall have document that will show ownership, role and responsibilities of departments /work process for applications developed like Website, fleet

management ,etc

### 21.4. Guidelines

#### 21.4.1. Third-Party Software Development (Outsourcing)

MOH has different types of experience on outsourcing software development to third parties on different time. The following are key measures that will be implemented during out sourcing.

- ICT development team should fully participate in the software development process.
- Contracted companies must design and develop the software inside MOH compound.
- ICT development team must assure a complete documentation is provided for any software developed by third party.
- ICT shall do the updating/upgrading of any software keeping in mind having standardized software utilization.
- User manuals must be designed and prepared for any software developed.
- The third party shall provide either TOT (Training of Trainers) or user training for concerned and appropriate staff before the software is deployed. This ensures proper testing and usage.

# 22. MOH Website

### 22.1. Overview

MOH has established a web presence over the internet for sharing up-to-date and reliable information to the public and the MOH community. Web hosting has become one of the services available on the MOH. This policy creates a standard way using MOH website.

### 22.2. Policy Statements

- MOH has a sole responsibility to manage the website, handle technical issues and provide training for end user.

- Public relation information process manages and follows up all the contents to be posted on the website.

22.3. Guidelines

**22.3.1. Responsibility**

- To enable the concerned work processes to publish their pages, ICT EO will provide disk space on web servers and training for relevant work processes.
- Work processes are responsible to assign dedicated personnel to post their content on the website.
- ICT EO will prepare and conduct the training on posting web content.
- The Public Relations shall review the content posting/publishing regularly and collect feedback from the website visitors.
- It is the responsibility of ICT EO to ensure that the policy is enforced as required and that the content posted on MOH's website adheres to the policy.

**22.3.2. Website Management**

- Public relation and ICT EO have the right to change or remove any information or link on the website to assure accuracy and timeliness.
- The website should be reviewed regularly.
- Time-sensitive content, such as information promoting events will be removed as soon as the event takes place.
- News should be reviewed and updated on a timely base.
- Links to other websites of similar mission will be provided on the site.
- All content on the website will adhere to applicable copyright and other laws.

**22.3.3. Website**

- The domain name of MOH's website is "www.moh.gov.et"

- Any technical inquiry about the web site should be sent to the following email address: **webmaster@moh.gov.et**
- MOH's website ownership should be clearly indicated on the homepage or directly accessible through a link from all other web pages.

### 22.3.4. Contingency Management (Backup)

- Web master of ICT will take Regular Back-up of the website and gives technical support.
- The website will be hosted on MOH's internal server.
- Should be included in disaster recovery infrastructure to ensure fastest restoration of the website in the event of any unforeseen hardware/software failure.

### 22.3.5. Web Content

- Content should be reviewed for quality (including originality, accuracy, and reliability) before posting.
- The website should provide information about MOH and other related topics.
- The content of MOH's website must include, among others**:**
  - Name and emblem of MOH
  - Mission, Vision and Goals of MOH
  - Aim and objectives of MOH
  - Organizational structure, including directorates, officers, etc
  - Contact address including Postal address, fax, phone number and email of the organization
  - MOH Press releases
  - Publications
  - Financial law, regulations & guidelines
- Any content on the website should be free of **:**

- Insulting, threatening or provocative language
- Inciting hatred on the basis of race, religion, gender, nationality or sexual orientation or other personal characteristics
- Swearing, using hate-speech or making obscene or vulgar statements
- Condoning illegal activity or breach of copyright
- Posting in a language other than the languages of the website
- Invading people's privacy

# 23. ICT Equipment Disposal

### 23.1. Overview

This policy is used for the ministry's IT equipment, often referred to as IT asset disposal (ITAD) or IT equipment recycling, which is a crucial aspect of information technology management. This procedure ensures data security, environmental responsibility, and compliance with regulations.

### 23.2. Purpose

The purpose of ICT hardware disposal is to manage the end-of-life cycle of ICT equipment in a responsible and environmentally friendly manner. This may involve various methods, including recycling, donation, resale, or secure destruction of equipment.

### 23.3. Policy Statements

This information communication technology (ICT) asset disposal policy is concerned with managing the secure disposal of equipment owned by the organization but no longer required.

### 23.4. Guidelines

To ensure the appropriate management of obsolescence and the disposal of ICT equipment, the following guidelines are in place:

a) **Determining Obsolescence**: The determination of obsolescence or the need for replacement of any ICT-related equipment will be made in collaboration with responsible bodies.
b) **Equipment Removal and Disposal:** The removal and disposal of any ICT equipment will be performed in collaboration with other responsible bodies *including knowledgeable individuals on equipment removal and disposal, compliance with environmental regulations.*
c) **Cannibalization of Hardware**: The ICT EO shall have sole responsibility for cannibalizing hardware that cannot be sold and can no longer be used as a whole but contains useful components. This allows for the salvage and reuse of valuable parts, minimizing waste and maximizing the utilization of resources.
d) **Data Security in Disposal**: The ICT EO must ensure that no equipment contains confidential, proprietary, or other sensitive information when disposed of, irrespective of the asset's value.
e) **Replacement of Old/Outdated Hardwar**e: To guarantee that the ministry utilizes a contemporary and efficient ICT infrastructure, it is necessary to replace hardware that has been in service for a minimum of five years and is considered outdated.
f) **Documentation of Hardware:** The ICT EO, in collaboration with respective EO will document the original purchase price to estimate and calculate depression cost. And usage of ICT hardware.

23.5. Policy management and Exception handling

#### 23.5.1. Non-Compliance

Violations of this policy may result in legal and administrative measures including termination of any agreements or termination of employment contract.

#### 23.5.2. Exception

a) Exceptions to this Policy should be approved by the minister of Health.
b) Any exceptions approved and implemented should be formally documented;
c) Policy exceptions should be reviewed on a regular basis (or as the need of the organization) for appropriateness;

#### 23.5.3. Review and update

This policy will be reviewed and updated every year or as deemed appropriate.

23.6. Enforcement

Individuals who do not comply with these policies shall be subjected to disciplinary action in accordance with IT policy and guidelines. Any disciplinary action under this policy shall consider the severity of the offense and the individual's intent. Disciplinary action can include revocation of privileges to use or access any or all components of the MOH Network Infrastructure.

In Large, the Violation of this policy shall be also addressed by appropriate MOH and Ethiopian Criminal /civic Code.