THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF HEALTH, COMMUNITY DEVELOPMENT, GENDER, ELDERLY AND CHILDREN

ICT Policy Guidelines

January 2016

THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF HEALTH, COMMUNITY DEVELOPMENT, GENDER, ELDERLY AND CHILDREN

ICT Policy Guidelines

January 2016

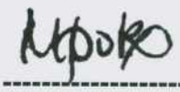
Foreword

The use of Information and Communication Technology (ICT) is essential in facilitating the Ministry's mission of ensuring availability and accessibility of quality healthcare services to all Tanzanians. It is thus imperative for the Ministry to acquire and maintain appropriate ICT infrastructure and services to improve the outputs of its key functions, hence serving society health needs as well as boost national social and economic development.

Succinctly, the purpose of the ICT policy guidelines document is to guide and enable the Ministry utilize ICT resources and expertise for the enhancement of quality administration, management and coordination of service provision. Thus, the policy guidelines shall assist in guiding appropriate development, deployment, maintenance, and use of ICT infrastructure and services at the Ministry, covering the following areas: ICT infrastructure acquisition, service level management, ICT acceptable use, software licensing, ICT assets management, ICT performance assessment, ICT maintenance and support, ICT security, disaster recovery and business continuity, and ICT risks management issues.

It is the responsibility of the ICT Department of the Ministry to foresee the implementation, management, monitoring and evaluation of the policy guidelines. On the other hand, ICT infrastructure and services users (staff, visitors/third party personnel) shall be responsible to abide to the guidelines stipulated in this document.

Lastly, the Ministry would like to extend a vote of thanks to all who were involved in one way or another in the realization of this important document.



Dr. Mpoki Ulisubisya
Permanent Secretary - Health
Ministry of Health, Community Development, Gender, Elderly and Children

Table of Contents

FOREWORD I

LIST OF ACRONYMS III

DEFINITION OF TERMS IV

1. PURPOSE AND CONTEXT 1

1.1 NATIONAL AND HEALTH SECTOR POLICIES RELEVANT TO ICT 1
1.2 SCOPE OF THE ICT POLICY GUIDELINES 2
1.3 OBJECTIVES 2
1.4 OUTCOMES OF THE POLICY GUIDELINES 3

2. POLICY GUIDELINES 4

2.1 ICT INFRASTRUCTURE ACQUISITION 4
2.2 SERVICE LEVEL MANAGEMENT 6
2.3 ICT ACCEPTABLE USE 7
2.4 SOFTWARE LICENSE MANAGEMENT 9
2.5 ICT ASSET MANAGEMENT 10
2.6 ICT PERFORMANCE ASSESSMENT 11
2.7 ICT MAINTENANCE AND SUPPORT 12
2.8 ICT SECURITY 12
2.9 BUSINESS CONTINUITY 18

3. POLICY GUIDELINES DOCUMENT STATUS 19

4. KEY STAKEHOLDERS 19

5. APPROVAL DETAILS 19

6. RELATED POLICIES AND DOCUMENTS 20

7. NEXT REVIEW DATE 20

8. ICT POLICY GUIDELINES OWNER 20

9. CONTACT PERSON 20

10. APPENDICES 21

10.1 ANNEX 1: ICT SERVICE DESK 21
10.2 ANNEX 2: ICT INCIDENT MANAGEMENT PROCESS 21
10.3 ANNEX 3: GUIDELINES FOR EVALUATING TOTAL COST OF OWNERSHIP (TCO) 21
10.4 ANNEX 4: GOODS INSPECTION AND ACCEPTANCE CHECKLIST 23
10.5 ANNEX 5: GUIDING PRINCIPLES FOR PASSWORD MANAGEMENT 24
10.6 ANNEX 6: ICT ASSET AND INVENTORY MANAGEMENT TEMPLATE 30

List of Acronyms

CCTV	Closed Circuit Television
eGA	Electronic Government Agency
HSSP IV	Health Sector Strategic Plan IV
ICT	Information and Communication Technology
MDG	Millennium Development Goals
NACP	National AIDS Control Program
NMCP	National Malaria Control Program
NSGRP	National Strategy for Growth and Reduction of Poverty
PPP	Public Private Partnership
SAN	Storage Area Network
SLA	Service Level Agreement
SLM	Service Level Management
SO	Strategic Objective
SOP	Standard Operating Procedure
SRS	System Requirements Specification
SSID	Services Set Identifier
TCO	Total Cost of Ownership
VIRP	Virus Incident Response Procedure
CDC	Centre for Disease Control
RTI	Research Triangle Institute
MUHAS	Muhimbili University of Health and Allied Sciences
JSI	John Snow Inc.
UCC	University Computing Centre
PO-PSM	President Office – Public Service Management
PO-RALG	President Office – Regional Administration and Local Government
NHIF	National Health Insurance Fund
NACP	National AIDs Control Programme
NMCP	National Malaria Control Programme
MSD	Medical Store Department
NTLP	National Tuberculosis and Leprosy Programme
NIMR	National Institute for Medical Research

Definition of Terms

i. **ICT Infrastructure** is a general term to encompass all ICT assets e.g. servers, workstations, storage, network, software, data, components, systems, applications, software licensing and resources. It is the sum of an organization's IT related hardware, software, data telecommunication facilities, procedures, documentations as well as policies, strategies and specifications that guide the effective use of these resources.

ii. **ICT Assets** are defined as equipment with central processing unit such as servers, network appliances, network storage devices, photocopier, scanner, computers, mobile devices, media player, digital cameras, audio-video recorders, large screen displays, projectors, amplifier, video or audio control units, but also include, and not limited to, software, functional support equipment and structure that are considered, part or as a whole, ICT solution.

iii. **ICT Security** is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

iv. **Computer Virus** is a piece of potentially malicious programming code that causes some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files or external storage media. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user.

v. **Electronic Mail** is a system of world-wide electronic communication in which a computer user can compose a message at one terminal that can be regenerated at the recipient's terminal when the recipient logs in.

vi. **Firewall** is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. The integrity of this protective barrier depends on the effective deployment, configuration and capabilities of individual firewall programs.

vii. **Software** is a collection of various kinds of programs that are used to operate computers and related devices.

viii. **Free and Open Source Software (F/OSS, FOSS)** is a software that is liberally licensed to grant the right of users to use, study, change, and improve its design

through the availability of its source code.

ix. **Proprietary Software** is software, licensed under exclusive legal rights of its owner.

x. **Hardware** is a comprehensive term for all of the physical parts of a computer, as distinguished from the data it contains or operates on, and the software that provides instructions for the hardware to accomplish tasks.

xi. **Intranet** is a private computer network that uses Internet Protocol technologies to securely share any part of an organization's information or operational systems within that organization, often protected from Internet traffic.

xii. **Information and Communication Technology (ICT)** refers to all those instruments, modes, and means through which information or data is captured, processed, stored and transmitted or communicated from one person to another or from place to place.

xiii. **Information Management System** is a computer program consisting of data storage systems, software and services, providing automated networked storage solutions) that lets one or more computer users create and access data in a database, having extensive transaction processing capabilities.

xiv. **Internet** is a computer network consisting of worldwide interconnected networks of computers that use the standard Internet Protocol (TCP/IP) to facilitate data transmission and exchange,

xv. **Total Cost of Ownership (TCO)** is a financial estimate intended to help buyers and owners determine the direct and indirect costs of a product, or system.

xvi. **Service Set Identifier (SSID)** is a case sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network (WLAN) that acts as a password when a mobile device tries to connect to the basic service set (BSS) -- a component of the IEEE 802.11 WLAN architecture.

xvii. **"The Ministry"** in this document is used to refer to the Ministry of Health, Community Development, Gender, the Elderly and Children.

xviii. **'ICT Department'** in this document is used to refer to the ICT department/unit of the Ministry, or the ICT department/unit of the Ministry's programmes, departments or agencies.

xix. **A Policy** is a statement or a set of statements defining a desired direction of operations or actions that define the interests and values of people it meant to serve. Statements are conceived to address a theme, or purpose of actions to society, institutions, and individuals, for present and future guidance.

xx. **A Policy Guideline** is any document and or statements that aim to streamline a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters and they define operationalization of the policy.

1. Purpose and Context

There is a growing evidence-based consensus that major advances in ICT have resulted in sweeping changes to the way healthcare services are managed and provided, and the way healthcare related information is collected, processed, stored and shared. Thus the health policy (2007) recognizes the potential and importance of deploying quality, efficient, user friendly ICT systems in order to increase performance levels and provide excellent services.

The Health Sector Strategic Plan (HSSP) IV clearly articulates the need to focus on strengthening ICT infrastructure and services in the health sector to ensure appropriate capacity exists to improve health outcomes for Tanzanians. This includes providing for future health-sector development through appropriate investment in information technology and communication systems.

In its efforts to actualize the use of ICT in the health sector, the Ministry launched the e-Health Strategy (2013 – 2018) that forms the basis for development of ICT infrastructure and applications of ICT to streamline and improve administrative processes (e.g. in planning and reporting) and for management of medical services (e.g. using electronic patient records). As part of the e-Health strategy implementation, the Ministry has put in place ICT infrastructure and services including local area network, various information systems, e-mail and web services, to mention just a few. However provision and management of these ICT services face a number of challenges such as:

- Lack of a clear understanding among Ministry staff of the roles of ICT department in terms of management of ICT infrastructure & services such as computers, information systems etc,
- Lack of procedures for vendor engagement on ICT equipment and services
- Lack of proper procedures for acquiring ICT services that may lead to equipment or services that do not meet standards
- Improper use of ICT services such as the use of other email services instead of using Ministry's email service.

The ICT policy guidelines document seeks among other things to address the aforementioned challenges and guide proper planning, development, deployment, use and management of ICT services at the Ministry. Consequently, the Ministry will be able to acquire appropriate ICT infrastructure and facilitate optimal deployment of ICT services, and ensure that ICT resources including facilities are used solely for the purposes for which they were intended.

1.1 National and Health Sector Policies Relevant to ICT

The Government has developed a number of enabling policies and environment as an effort to strengthen the health services in Tanzania. Enabling policies are both

national and international commitments. The ICT policy guidelines document intends to implement the following national and health sector policies relevant to ICT:

National ICT Policy 2003: Emphasizes on the use of ICT to enhance and improve the quality and efficiency of healthcare service delivery.

National Health Policy 2007: The ICT policy guidelines implement the national health policy which emphasizes on using ICT to increase productivity, efficiency and quality of health care in the country.

The National Development Vision 2025: Seeks to promote use of ICT for competitive social and economic transformation.

e-Government Agency (eGA) ICT Management Standards and Guidelines: Stipulates the need for all public sectors to put in place ICT policy guidelines.

Health Sector Strategic Plan of 2016-2020 (HSSP IV): Seeks to embrace rapid development of ICT for improving administrative and management processes, patient/client recording and communications.

1.2 Scope of the ICT Policy Guidelines

The ICT policy guidelines address issues related to hardware and software, data and associated methodologies, infrastructure and devices that are operated, connected, used or brought onto the Ministry of Health, Community Development, Gender, Elderly and Children headquarter, health programs, departments and agencies.

Furthermore, the ICT policy guidelines applies to all staff at the Ministry headquarter; health programs, departments and agencies, consultants, researchers, visitors as well as institutions that make use of the Ministry ICT infrastructure and services. The targeted health programs, departments and agencies include National AIDs Control Programme (NACP), National Malaria Control Programme (NMCP), Immunization and Vaccination Development (IVD), National Health Insurance Fund(NHIF), National Blood Transfusion Services(NBTS), Tanzania Food and Drugs Authority (TFDA), Medical Stores Department (MSD), Tanzania Food and Nutrition Center (TFNC), Reproductive and Child Health Services (RCHS), National Tuberculosis and Leprosy Programme (NTLP), to mention just a few.

1.3 Objectives

The objective of the policy guidelines document is to ensure that all ICT infrastructure and services are properly managed and utilized to support the Ministry achieve its core vision of "*having a healthy society with improved social well being that will contribute effectively to individual and national development*".

Specific objectives:

- To ensure compliance to government standards and procedures during acquisition and implementation of ICT infrastructure and services;
- To provide equitable access to ICT services to the Ministry staff and other stakeholders;
- To provide adequate information to the Ministry staff on proper use of ICT facilities;
- To ensure the integrity, reliability, availability, efficiency and superior performance of ICT systems;
- To ensure that use of ICT systems is consistent with the principles and values that govern use of other Ministry facilities and services;
- To ensure that ICT systems are used for their intended purposes; and
- To facilitate strengthening of ICT infrastructure to support and enhance healthcare service provision.

1.4 Outcomes of the Policy Guidelines

- Improved ICT service provision and use at the Ministry
- Strengthened ICT security and confidentiality
- Proper management of ICT assets life cycle at the Ministry
- Properly managed risks associated with the use of ICT at the Ministry
- Improved health outcomes due to improved use of ICT to support the core functions of the Ministry
- Empowered staff and other stakeholders on the optimal and ethical use of ICT facilities and services at the Ministry
- Improved efficiency and effectiveness of administration and management related activities at the Ministry

2. Policy Guidelines

The ICT policy guidelines are presented in nine thematic areas: ICT Infrastructure Acquisition, Service Level Management, ICT Acceptable Use, Software Licensing, ICT Asset Management, ICT Performance Assessment, ICT Maintenance and Support, ICT Security, and Business Continuity.

2.1 ICT Infrastructure Acquisition

2.1.1 Purpose

To guide consistently the acquisition of ICT infrastructure, systems and services within the Ministry headquarter, health programmes, departments and agencies to ensure compliance with the ICT standards, specifications and guidelines approved by the responsible government authorities.

2.1.2 Scope

It applies to the acquisition of all ICT infrastructure, systems and services, through different means including public procurement, Public Private Partnership (PPP) and in kind or donor support.

2.1.3 Procedures for acquisition of hardware

2.1.3.1 The ICT department shall prepare and publish updated standards and specifications as and when they are realized and shall advise users accordingly.

2.1.3.2 ICT department shall receive and review user requirements for procuring ICT equipment and ensure compliance with standards and business needs.

2.1.3.3 A total cost of ownership (TCO) shall be evaluated using the Ministry guidelines (Annex 3) prior to acquisition of any ICT hardware or system.

2.1.3.4 ICT department shall inspect and verify the procured ICT infrastructure and services to ensure conformity to the set ICT standards and specifications prior to acceptance by the users.

2.1.3.5 All ICT infrastructure and service donations should be communicated to ICT department before delivery or shipping to ensure compliance to the ICT standards, guidelines ad specifications.

2.1.3.6 ICT department shall ensure the procured or acquired goods are registered and status updated periodically in the ICT inventory.

2.1.3.7 ICT department shall ensure the ICT Infrastructure and services are monitored, evaluated and maintained.

2.1.3.8 Ministry departments and agencies through their ICT units/departments shall submit their plan/proposal for acquisition of data centre/server equipment for review by the Ministry ICT department.

2.1.4 Procedures for acquisition of software and respective services

2.1.4.1 The following are the procedures that shall apply in the acquisition of software or information systems, and services.

2.1.4.2 All user requirements (functional & non functional requirements) for procuring software shall be reviewed by ICT Department to ensure compliance with the Ministry standards and business needs.

2.1.4.3 ICT department in collaboration with user department shall conduct a feasibility study or business needs assessment before acquisition of software or system.

2.1.4.4 ICT and user departments shall develop detailed requirements for the software intended to be procured which shall include functional and non functional requirements.

2.1.4.5 A total cost of ownership (TCO) shall be evaluated prior to acquisition of software (Refer annex 3 for guidelines).

2.1.4.6 ICT department shall ensure that any acquired information system software is compliant to the Ministry Health Information Exchange (HIE) standards, and therefore able to exchange and share data through the Health Information Mediator (HIM).

2.1.4.7 ICT department of the Ministry headquarter shall consult institution responsible with e-Government compliancy for approval in software acquisition process to ensure compliance to e-Government Interoperability Framework (e-GIF) and other related e-Government guidelines1.

2.1.4.8 ICT department shall ensure adherence to the chosen methodology of software development throughout the entire process of acquisition of software.

2.1.4.9 For any Ministry project targeting in-house development and or outsourced development/customisation of software system solution, the ICT department shall ensure before project closure developers/suppliers provides detailed documentations, both technical documentation and operating user manual.

2.1.4.10 ICT and user departments shall inspect, test and certify all ICT systems (new or existing), to ensure that they conform to the set ICT standards, guidelines and specifications.

2.1.4.11 ICT department shall ensure the software and respective licences are registered in the ICT inventory as per software licence management policy guidelines.

2.1.4.12 The ICT department shall develop an evaluation and maintenance plan for the procured goods as per ICT maintenance and support policy guidelines.

2.1.4.13 The ICT department shall ensure that the ICT security policy guidelines are adhered to during hardware, network and information system acquisition and development.

2.1.4.14 Ministry departments and agencies through their ICT units/departments shall submit their plan/proposal for procurement of any information system software or any software license for review by the Ministry ICT department.

---

[1] Guide for Appropriate, Proper and Safe Use of Information and Telecommunication Technology Equipment in the Government, second edition, 2015, PO-PSM.

2.1.5 Procedures for Disposal of Equipment

2.1.5.1 ICT department shall be responsible to inspect periodically or on demand all obsolete ICT infrastructures and advise procurement management unit for disposal.

2.1.5.2 The ICT department shall ensure important data from obsolete or decommissioned ICT equipment is backed up and archived.

2.1.5.3 ICT department shall ensure there is a secure mechanism to erase sensitive information before disposing of ICT equipment as per Government guidelines governing disposal of ICT assets.

2.2 Service Level Management

2.2.1 Purpose

The Ministry acquires and uses service of third party hardware, system or service providers. All ICT services outsourced shall have Service level agreements (SLA) or service contracts. This may include but not limited to Internet and data connectivity service providers, maintenance and repair services, system configuration and other related short / long term services. This section therefore provides guidance on how internal and external service levels shall be managed.

2.2.2 Scope

This covers all ICT infrastructure and services provided to the Ministry headquarter, programmes, departments and agencies by service providers.

2.2.3 Procedures

2.2.3.1 The Ministry headquarter, programmes, departments and agencies shall enter into and maintain service level agreements with all ICT service providers.

2.2.3.2 SLAs or service contracts shall form a basis for performance appraisal of the respective providers, and also form a basis for their payment or compensation.

2.2.3.3 The ICT department/Units shall continuously monitor the Service level parameters and ensure they don't fall below the agreed standards.

2.2.3.4 All service level agreements or service contracts must comply with security policy guidelines and standards; and shall be in accordance to the public procurement laws, regulations and guidelines

2.2.3.5 All SLAs or service contracts between donor and service providers shall be reviewed and approved by the ICT department at the Ministry headquarter.

2.2.3.6 The copy of approved SLA or contract shall be retained by the Ministry for monitoring purposes.

2.2.3.7 The ICT department/units shall monitor the service level agreement performance and record, report and escalate any support problems causing interruptions to service.

2.3 ICT Acceptable Use

2.3.1 Purpose

To identify proper usage and behavior of the Ministry ICT infrastructure and services, with the overall aim of protecting the rights and privacy of all employees, and the integrity and reputation of the Ministry. ICT facilities provided to employees shall be used solely for the Ministry business purposes.

2.3.2 Scope

2.3.2.1 This applies to all employees of the Ministry headquarter, programmes, departments and agencies. The principles of the policy guidelines will also be applied, as far as is reasonably practicable, to non-employees working at Ministry/establishment locations and making use of Ministry/establishment ICT systems (e.g. facilities users, technical assistants, Council members, contractors, visitors).

2.3.2.2 ICT facilities encompass (but are not restricted to) the following services provided by the Ministry and third parties on its behalf:

a. Network infrastructure, including (but not exclusively) the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers;
b. Network services, including (but not exclusively) Internet access, web services, email, wireless, messaging, shared file store, printing, telephony and fax services, CCTV, and door access control;
c. Ministry owned or leased computing hardware, both fixed and portable, including (but not exclusively) personal computers, workstations, laptops, tablets, PDAs, mobile devices, smartphones, servers, printers, scanners, disc drives, monitors, keyboards and pointing devices;
d. Software and databases, including applications and information systems (DHIS, HRHIS, PlanRep, Epicor, HFR, TIIS, etc), videoconferencing environments, ICT laboratories, software tools, and information services.

2.3.3 Acceptable Use Principles

All users of the ICT facilities must comply with the following principles:

2.3.3.1 Users shall use the ICT facilities and access to the Internet in a responsible manner in accordance with this guideline and all applicable laws in the Government of Tanzania. If Users are in any doubt about

what constitutes acceptable use according to this guideline, they should seek guidance from the ICT department.

2.3.3.2 Users shall comply with regulations and policies issued by the government and other relevant copyright legislation, licences and agreements for software and electronic information resources when accessing and connecting to Ministry ICT facilities.

2.3.3.3 Each user shall be issued with a valid username and password which must be used to authenticate and gain access to the ICT facilities. Users shall be responsible for all activities that take place under their usernames.

2.3.3.4 Access to the ICT facilities using someone else's username and password is prohibited. Passwords shall meet the Password complexity requirement as stipulated in the password users' guidelines (Annex 5).

2.3.3.5 All employees shall utilise the Ministry provided email accounts as the official mechanism for email communication.

2.3.3.6 ICT department shall utilise best information security and management practices for the storage, access, retention and deletion of Ministry information.

2.3.3.7 The Ministry shall make use of government owned storage/hosting environment and the use of other cloud computing services that will need to be negotiated and approved by e-Government Agency shall be considered as a fall-back position.

2.3.3.8 All users shall obtain authorisation for purchasing / obtaining software licences and for installing software on Ministry owned computers from ICT department (via the ICT Service Desk).

2.3.3.9 Staff shall obtain permission from the ICT department in case there is a requirement to move computing equipment from one location to another.

2.3.3.10 Users should make all reasonable efforts to send data that is 'virus free' and not open email attachments or click on links sent by unsolicited or un-trusted sources.

2.3.3.11 Users accessing Ministry ICT facilities using their own computing devices shall ensure that they have updated operating systems & anti-virus programs.

2.3.3.12 The ICT department shall ensure that all information systems and supporting infrastructure comply with the ICT Policy guidelines and current legislations.

2.3.3.13 Users will be solely responsible for all claims, liabilities, damages, costs and expenses suffered or incurred by the Ministry which result

from their use of the ICT facilities in contravention of this Policy guideline;

2.3.3.14 Users shall report any technical problems, requests or concerns regarding a suspected policy guidelines breach directly to the ICT Department.

2.3.4 Procedures

The ICT department shall ensure that:

2.3.4.1 All emails, internet use, and other ICT usage is logged to facilitate Investigation or detection of unauthorized use of the Ministry's ICT facilities and ensure compliance with this policy guideline and other regulations.

2.3.4.2 ICT activity logs retention schedule is place, and that records of all ICT activity are retained in accordance with the ICT retention schedule. ICT activity logs shall also include access to Ministry ICT facilities when using personally owned computers or mobile devices. Any monitoring shall be proportionate to the assessed risk to Ministry ICT infrastructure and information systems.

2.3.4.3 Tools used to protect the Ministry ICT infrastructure may include (but are not limited to) use of historical log/logging files, print audit software, filtering software to limit browsing of inappropriate sites and downloads, automatic checking of emails and attachments for viruses; blocking of some telephone numbers and deletion of certain files and emails deemed appropriate by the Ministry's Head of ICT.

2.3.4.4 ICT items that are Ministry owned or leased computing equipment/device connected to the network shall be inspected to ensure that it is removed from the network if it is deemed to be breaching the ICT policy or otherwise interfering with the operation of the network.

2.3.4.5 Information security events and actual or suspected breaches of this policy guideline should be reported immediately to the Ministry ICT Service Desk.

2.4 Software License Management

2.4.1 Purpose

To ensure that software licences within the Ministry are effectively recorded, managed and controlled. The policy guideline intends to promote sharing of software licenses across the Ministry.

2.4.2 Scope

It applies to management of software licenses at the Ministry headquarter, programmes, departments and agencies.

2.4.3 Procedures

2.4.3.1 The ICT Department shall:

2.4.3.2 Ensure that all software licenses purchased and deployed are collected and recorded as per the ICT assets management policy guidelines.

2.4.3.3 Implement network scanning tools to detect any unauthorized or unlicensed installed software.

2.5 ICT Asset Management

2.5.1 Purpose

The Ministry is committed to manage the lifecycle of its ICT assets. This policy guideline provides the overall framework for the management of ICT assets from procurement to disposal.

2.5.2 Scope

It applies to all ICT assets owned by the Ministry headquarter, programmes, departments and agencies.

2.5.3 Procedures

The ICT Department shall:

2.5.3.1 Conduct audit of the ICT assets location and update the inventory accordingly as per ICT inventory sheet (Annex 6).

2.5.3.2 Put in place and maintain ICT inventory management system with barcode labelling and scanning devices.

2.5.3.3 Update and maintain the accuracy of the ICT inventory management system when ICT assets moves, or are disposed, etc.

2.5.3.4 Ensure that ICT asset is signed for (without amendment) by asset holders and declaration is scanned into the ICT inventory management system.

2.5.3.5 Apply ICT supplied barcode asset tag before ICT asset is taken out of procuring office.

2.5.3.6 Check ICT asset is returned in the same configuration as expected and signing return form upon collection from the asset holders;

2.5.3.7 Ensure barcode asset tags are assigned to all purchased ICT equipment.

2.5.3.8 Review all ICT assets before disposal.

Users shall:

2.5.3.9 Ensure loss or theft of ICT asset is reported with evidence immediately to the ICT Department and marked as lost or stolen in the assets inventory

2.5.3.10 Ensure all ICT assets are returned to ICT Department upon replacement or equipment redundancy.

2.5.3.11 Ensure as ICT equipment holders retain responsibility for equipment issued to them until it has been returned to ICT Department for redeployment or disposal;

2.5.3.12 Not conduct repair or maintenance of any ICT asset without written permission from the ICT department

2.5.3.13 Ensure Fixed ICT asset are not moved without consultation with the ICT Department.

2.5.3.14 Be aware that ICT asset may be requested for auditing at any time

2.6 ICT Performance Assessment

2.6.1 Purpose

ICT Performance assessment intends to support the Ministry to measure progress towards implementation of the ICT policy guidelines and/or e-Health strategic plan in the Ministry. By carrying out accurate performance assessment immediate corrective measures can be put in place to prevent problems from arising, as well as providing a basis for the Ministry top management to commit resources to address impending problems.

2.6.2 Scope

The ICT performance assessment covers all the Ministry ICT policy guidelines and strategies addressing design, development, implementation and use of ICT infrastructure and services.

2.6.3 Procedures

2.6.3.1 The head of ICT department shall form 'ICT performance assessment taskforce' to conduct regular ICT assessment.

2.6.3.2 The ICT performance assessment taskforce shall develop a comprehensive assessment tool covering all the key aspects of Ministry ICT policies and strategic goals implemented under the ICT department.

2.6.3.3 The performance assessment tool shall be pre-tested to ensure completeness in terms of the areas covered.

2.6.3.4 The ICT performance assessment taskforce shall conduct the assessment exercise at least once a year. A comprehensive

assessment report shall be prepared and shared with the Ministry management for action.

2.6.3.5 The ICT performance assessment tool shall be reviewed annually or any time deemed necessary to do so.

2.7 ICT Maintenance and Support

2.7.1 Purpose

To provide a framework for maintenance and support of ICT services to ensure smooth and efficient ICT services. It is also meant to streamline the way in which support requests are reported, logged and resolved. The ICT department shall provide timely and appropriate support and maintenance services to all authorised users of all ICT facilities owned by the Ministry headquarter departments and agencies.

2.7.2 Scope

It covers maintenance and support of computing infrastructure and business applications including installation, configuration, training, usage, upgrades, and updates, preventive and corrective maintenance.

2.7.3 Procedures

The ICT department shall:

2.7.3.1 Establish ICT service desk to provide a point of contact where end users can report incidents and obtain assistance with the use of ICT services Refer Annex 1: Ministry ICT Service Desk.

2.7.3.2 Put in place a comprehensive incident management system to address ICT related incidents within the Ministry.

2.7.3.3 Put in place the ICT client services charter and ensure its proper implementation.

2.7.3.4 Perform preventive and corrective maintenance of ICT infrastructure and services at least twice a year.

2.8 ICT Security

2.8.1 Purpose

ICT security policy guidelines aim at protecting the Ministry ICT computing infrastructures, software, data from unauthorized access, hazards, intentional or unintentional damage as well as theft in conformity with international best practices, National ICT policy, National e-Government strategy, standards and guidelines. Breaching of the security policy guidelines can lead to the loss or compromise of confidentiality, integrity, accessibility and availability of information systems assets.

2.8.2 Scope

The ICT security policy guidelines target to protect Ministry's ICT infrastructure and services from unauthorized access, hazards, intentional or unintentional damages as well as theft. It applies to the Ministry Departments, programs, agencies and all others granted to use Ministry's ICT infrastructure and services.

2.8.3 ICT infrastructure Security

The Ministry shall secure all ICT infrastructures and implement security controls in conformity with international best practices, National ICT Policy, National e-Government Strategy, standards and guidelines.

2.8.3.1 Procedures

2.8.3.1.1 ICT Department shall advise the Ministry on the appropriate equipment and software for securing ICT infrastructure and services.

2.8.3.1.2 ICT department shall assess and evaluate the conformity of the security tools to the international best practices, National ICT Policy, National e-Government strategy, standard and guidelines.

2.8.3.1.3 ICT Department shall be responsible for day to day management of the security of the computing infrastructure.

2.8.3.1.4 ICT department shall report security breach to the Ministry management for actions.

2.8.4 Privacy and Integrity

The Ministry shall ensure that the privacy and integrity of all users of the Ministry's ICT infrastructure and services are enforced and respected by all.

2.8.4.1 Procedures

The ICT department shall monitor and ensure that:

2.8.4.1.1 Users shall respect the privacy and integrity of other users' information assets.

2.8.4.1.2 No staff shall be allowed to view, copy, alter or destroy another person's electronic files without owner's permission.

2.8.4.1.3 ICT Department shall designate one personnel who shall occasionally monitor information on the network and/or computer systems to maintain and ensure the integrity of the systems.

2.8.4.1.4 The ICT Department shall be responsible for managing and monitoring users operations in order to maintain and protect the integrity, security and functionality of ICT resources.

2.8.4.1.5 Systems and Network Administrators shall respect the privacy and integrity of personal communications in all forms including telephone, electronic mail and file transfers.

2.8.5 Confidentiality and Data Integrity

The Ministry shall protect data to ensure confidentiality and integrity.

2.8.5.1 Procedures

2.8.5.1.1 ICT Department shall take all necessary steps to prevent unauthorized access to confidential information.

2.8.5.1.2 The Ministry shall classify information according to sensitivity. Access and handling of information classified as confidential shall be limited to authorized personnel and shall be controlled through appropriate administrative and technical standard operating procedures.

2.8.5.1.3 ICT department shall take reasonable steps to protect unauthorized entry into users' accounts or files. ICT Department shall ensure that only relevant and appropriate data and information are retained on Ministry servers for the maximum length required as per legal, standards and guidelines for government archives rules.

2.8.5.1.4 ICT Department shall not be responsible for data loss in the personal computers or system; this shall be the responsibility of the owners.

2.8.6 Physical Security

The Ministry shall ensure that physical access to ICT infrastructure are controlled and secured.

2.8.6.1 Procedures

The Ministry and ICT Department shall:

2.8.6.1.1 Ensure Server rooms, Computer rooms and Disaster Recovery Sites are physically protected against unauthorized access using secure door locks with password, biometric or access control card, CCTV cameras or other electronic locks.

2.8.6.1.2 Ensure that security measures such as Fire extinguisher, smoke detectors are in place to prevent disasters.

2.8.6.1.3 Ensure Physical access to ICT equipment such as servers, routers, switches, computers labs and others is strictly granted to only authorized individuals.

2.8.6.1.4 Ensure that any staff/visitors authorized to enter the server or computer rooms are accompanied by ICT officer responsible and visitors shall be logged in the register book.

2.8.6.1.5 Provide guidance to all staff on how to observe access procedures and those whom their access rights are withdrawn shall return their ID cards and system access privileges/credentials to Permanent Secretary- of the Ministry.

2.8.6.1.6 Ensure that all staff/workers are responsible for safeguarding the equipment entrusted to them by the Ministry. This includes reasonable protection of equipment from damage and theft.

Users shall:

2.8.6.1.7 Be responsible for damage or loss of computers or other electronic assets caused by negligence, or recklessness.

2.8.6.1.8 Not tamper with the Ministry ICT property.

2.8.7 Logical Security

The Ministry shall ensure that only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights.

2.8.7.1 Procedures

The Ministry and ICT Department shall:

2.8.7.1.1 Ensure that all employee, persons or entities are registered and uniquely identified, authenticated and authorized before access is granted to the Ministry information and systems. There should be a formal procedure for revoking access to all information systems and services in case an employee/ a user leave the Ministry in the event of retirement, etc.

2.8.7.1.2 Ensure access privileges are granted only to the minimum level required by the user's role, on principle of "need-to-know" and need-to-do" basis in accordance with user's job responsibilities, business and security requirements.

2.8.7.1.3 Ensure that the information resources and business application access right are reviewed periodically (at least every three months.) for unused, redundant, or expired user accesses or accounts, or incorrect privileges. Special attention should be given to privileged access rights, which allow users to override system controls.

2.8.7.1.4 Ensure that user data stored on computer local hard drives and should be automatic backed up on network storage server or network files servers. This shall ensure that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

2.8.7.1.5 A formal record of all registered users shall be maintained by the ICT Department and checked periodically (at least every three months) for unused, redundant, or expired user accesses or accounts, or incorrect privileges.

2.8.7.1.6 The ICT Department shall ensure that mechanisms are place to prevent unauthorised personnel, remote connections and other system (network)

entry ports from accessing computer resources and minimize the need for authorised users to use multiple sign-on.

2.8.7.1.7 Ensure that access rights are strictly limited, particularly to temporary staff and contractors, to a need-to-know basis that permits access only to the systems and resources that are required for them to perform their duties.

2.8.7.1.8 Ensure procedures are defined for the allocation of passwords (both permanent and temporary) to users in a secure and confidential manner in compliance to the password Guideline. Refer Annex 5.

2.8.7.1.9 Ensure that the use of removable media which are not property of the Ministry is prohibited unless authorized by line management and the head of ICT department.

User shall:

2.8.7.1.10 Be responsible for all transactions made under the authorization of his or her ID and password, and for all network activity originating from that connection.

2.8.7.1.11 Ensure that they log off and shut down, if they expect to be away from their desk or work area for a prolonged period and at the end of the working day before they leave office premises.

2.8.8 Network Security

The Ministry shall ensure internal networks and systems are adequately protected against any threats from external or internal sources that could disrupt operations or gain unauthorized access to the Ministry network and services. These guidelines will help to protect resource and integrity of computing network.

2.8.8.1 Procedures

The Ministry through ICT Department shall:

2.8.8.1.1 Ensure that the Local Area network is logically separated to help traffic management, segregation of incompatible duties and access privileges of both internal and external users.

2.8.8.1.2 Ensure authorized external sources or users outside of the Ministry network are appropriately identified and authenticated before their session connected into the Ministry network.

2.8.8.1.3 Ensure that network ports that permit remote access for administrators or diagnostic use have appropriate security mechanisms to prevent unauthorized access.

2.8.8.1.4 Ensure access capabilities of users connecting across the shared network are limited according to their nature of works, roles and privileges.

2.8.8.1.5 Ensure that network services, remote and external connections to the network (including diagnostic ports) should be centrally controlled and the

access privileges provided should be limited to those services required for business purposes.

2.8.8.1.6 Ensure that all network logons are authenticated with unique user ID and password to ensure that only authorised users gain access to the network.

2.8.8.1.7 Ensure that the Ministry network addressing structure and other directory information are protected by firewall.

2.8.8.1.8 The designated system administrator should develop a coverage map of the wireless network, including locations of respective access points and services set identifier (SSID) so as to avoid overlapping of wireless signal.

2.8.8.1.9 ICT Department reserves the right to turn off without notice any access port to the network that puts the organization's systems, data, users, and clients at risk.

2.8.8.1.10 The ICT Department reserves the right to audit any portable computer used for Ministry business to ensure that it continues to conform to this policy; also it reserves the right to deny network access any laptop or computer which has not been properly configured and certified complying with this policy.

2.8.9 Virus Protection

The Ministry shall maintain a corporate antivirus for use to Ministry-owned computers.

2.8.9.1 Procedures

2.8.9.1.1 The user shall ensure that any virus detected shall be report to ICT department with the following information (if known): Virus name, extent of infection, source of virus, and potential recipients of infected material.

2.8.9.1.2 ICT department shall ensure that any virus-infected computer or suspected computing devices will be removed from the network until it is verified as virus-free.

2.8.9.1.3 ICT department shall enable real time detection to scan computer virus and malicious code, for active processes, executable and documents files that are being processed.

2.8.9.1.4 Users shall ensure that any files on electronic or optical media, or file receive over network including emails are scanned against computer virus and malicious codes before open or use.

2.8.9.1.5 ICT department shall communicate new virus alert to warn the users about the incident and appropriate measures and response.

2.8.9.1.6 ICT department shall put the guideline for Virus Incident Response Procedure (VIRP).

2.8.9.1.7 The ICT department shall be responsible for network, Internet and email security control mentioned above.

2.9 Business Continuity

2.9.1 Purpose

This is an essential part of the Ministry response planning for ICT disaster management. It sets out mechanisms for disaster preparedness and how the business will operate following an incident and how it expects to return to business as usual in the quickest possible time. Furthermore, the policy seeks to provide a reliable approach for identifying ICT risks occurrence and their effects on the Ministry services delivery

2.9.2 Scope

It covers backup and restoration of data, disaster recovery, risk management, emergency preparedness and response within the Ministry headquarter, programmes, departments and agencies.

2.9.3 Disaster Preparedness and Recovery

The Ministry shall ensure that ICT disaster preparedness and recovery plan is in place, as a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services; and is planned to result in a more resilient and reliable ICT services.

2.9.3.1 Procedures

2.9.3.1.1 The ICT department shall develop a disaster recovery plan document for handling ICT services. Among other things, the plan shall include the following information:

i. Real time backup in of all critical information system
ii. Backup and restoration to be regularly tested as per backup and restoration procedures
iii. Backup and restoration process to be done using central government data centre
iv. Backup roster and responsible person to do backup and a supervisor to verify the backup

2.9.3.1.2 ICT department shall test the disaster recovery plan at least twice a year to ensure that it is functioning and the result reports are documented.

2.9.3.1.3 ICT department shall orient the disaster recovery plan to other department users.

2.9.3.1.4 ICT department shall review the disaster recovery plan once a year.

2.9.4 Risk Management

The Ministry shall ensure that risk management procedures are in place and implemented so that in the event of an incident or disaster, business continues

2.9.4.1 Procedures

The ICT department shall:

2.9.4.1.1 Prepare and annually review an ICT risks assessment checklist tool.

2.9.4.1.2 Conduct risks assessment exercise using the risks assessment checklist at least once every year.

2.9.4.1.3 Prepare ICT the risk management register using the information collected during risks assessment.

2.9.4.1.4 Review the ICT management register at least once every year.

2.9.4.1.5 Put risk management activities in the overall ICT strategic plan and set aside resources for risks mitigation.

3. Policy Guidelines Document Status

This is a new ICT policy guidelines document.

4. Key Stakeholders

4.1. The stakeholders who were involved in the realization of this policy guidelines document include the following:

i. Ministry of Health, Community Development, Gender, the Elderly and Children headquarter, units and department
ii. Other Ministries: POPSM and PO-RALG.
iii. University institutions: UCC, and MUHAS.
iv. Ministry agencies and departments: NHIF, NACP, NMCP, TB/LP, MSD, and NIMR.
v. Development partners: CDC, RTI and MCSP/JSI.

4.2. The main stakeholders of this policy guidelines document include:

i. All Ministry of Health, Community Development, Gender, Elderly and Children headquarter staff
ii. All the Ministry departments and agencies
iii. All Ministry health programmes
iv. Any other stakeholders using ICT facilities at the Ministry headquarter, health programmes, departments and agencies.

5. Approval Details

The policy guidelines document was approved by the Ministry of Health, Community Development, Gender, Elderly and Children at the meeting held on.....**(Approval Date).**

6. Related Policies and Documents

i. Tanzania's National ICT Policy of 2003,
ii. e-Government Agency (eGA) ICT management standards and guidelines
iii. Tanzania National Health Policy (1990, 2003 and 2007 Revisions)
iv. Health Sector Strategic Plan (HSSP) IV
v. Tanzania e-Health Strategy 2013-2018
vi. Tanzania Development Vision 2025,
vii. National Strategy for Growth and Reduction of Poverty (NSGRP),
viii. Sustainable Development Goals (SDGs)

7. Next Review Date

The Ministry ICT policy guidelines document shall be reviewed after every three years or when deemed necessary to assess the effectiveness of its implementation and determine policy areas that need to be revised. The periodic review shall ensure the policy guidelines document is in line with the Ministry changes that might have taken place.

8. ICT Policy Guidelines Owner

The Ministry of Health, Community Development, Gender, Elderly and Children, under ICT department is the owner of this ICT policy guidelines document.

9. Contact Person

The contact person for issues related to the ICT policy guidelines is:

Head, Information and Communication Technology (ICT)
Ministry of Health, Community Development, Gender, Elderly and Children
6 Samora Machel,
P.O.BOX 9083,
11478 Dar es Salaam,Tanzania.

10. Appendices

10.1 Annex 1: ICT Service Desk

Aims

- To provide an effective and efficient first point of contact for the Ministry workforce and shared service partners to access ICT facilities and support.
- To provide an efficient and effective first and second line support service with the aim of restoring services at the earliest opportunity to maximize productivity of employees and users.

Service Desk Location

The service desk will be split into various physical locations, although it will function as a central service desk. The locations will include the Ministry HQ, NACP, and NMCP. The NACP and NMCP will provide support for their users at first line for specialist services and applications. However, if any user from a NACP/NMCP calls the IT service desk at HQ, the request will be logged and passed to NACP and NMCP IT personnel for resolution.

Service Desk Interaction

There will be three ways to interact with the service desk and these are through: email, telephone or web. The service desk operates from 08.00am to 17.00pm Monday to Friday in all the locations and from 09.00am to 15.00pm on Saturdays and Sundays in only one location (the Ministry HQ).

10.2 Annex 2: ICT Incident Management Process

If there is any incident occurrence the following process shall be followed:

i. Log all incident/service request details, and allocate categorization and prioritization codes.
ii. Provide first line investigation and diagnosis.
iii. Resolve incidents/service requests that do not need escalating to Service Support (second line).
iv. Escalate incidents/service requests that the service desk cannot resolve within 1hr timescale.
v. Close all resolved incidents, service requests and other calls.
vi. Conduct customer/user satisfaction call backs/surveys
vii. Communicate with users – keeping them informed of incident progress, notifying them of impending changes or agreed outages, etc.
viii. Update the configuration management system under the direction and approval of configuration management if so agreed.

10.3 Annex 3: Guidelines for evaluating Total Cost of Ownership (TCO)

The following factors shall be considered for evaluation:

1. Acquisition Expenses

i. Software licensing
ii. Hardware (server, client workstations, mobile devices)
iii. Infrastructure (networking hardware and software)
iv. Human resource requirements
v. Technical support for installation and configuration costs
vi. Initial training costs

2. Operational (Ongoing) expenses
   i. Software support – Configuration changes and version updates
   ii. Training costs
   iii. Migration costs. Should it ever become necessary to move to another vendor or system then the data within the system should be easy to export to a standard open formats e.g. csv, etc.

10.4 Annex 4: Goods Inspection and Acceptance Checklist

1.	**Supplier**							
2.	**LPO. No**							
3.	**Invoice No.**							
4.	**Delivery Note No.**							
5.	**Amount**							
6.	**User Department**							
7.	**Goods Specifications**	**Type**	**Model**	**Operating system**	**Office Pkg**	**Warrantee**	**Antivirus**	**Serial Number**
8.	**Goods Accepted? (YES/NO)**							
9.	**Remarks**							
10	**Inspected By (ICT Officer)**	**Name** .....**Signature** ..... **Designation** .....**Date**						
11	**Received By (PMU Officer)**	**Name** .....**Signature** ..... **Designation** .....**Date**						

10.5 Annex 5: Guiding Principles for Password Management

This guideline applies to all staffs that have a username and password to use in at least one system or application at the Ministry headquarter, health programmes, departments and agencies, independent of whether you are an end user or a system administrator.

A Strong Password is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

Guidelines for creating a Strong Password:

i. Be at least 8 characters in length
ii. Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
iii. Have at least one numerical character (e.g. 0-9)
iv. Have at least one special character (e.g. ~!@#$%^&*()_-+=)

A Strong Password should not -

i. Spell a word or series of words that can be found in a standard dictionary
ii. Spell a word with a number added to the beginning and the end
iii. Be based on any personal information such as user id, family name, pet, birthday, etc.

How to Maintain a Strong Password:

i. Do not share your password with anyone for any reason
ii. Change your password periodically
iii. Consider using a passphrase as a hint instead of a password
iv. Do not write your password down or store it in an insecure manner
v. Avoid reusing a password
vi. Avoid using the same password for multiple accounts
vii. Do not use automatic logon functionality

Guiding Principles for Systems Administrators:

i. Enforce strong passwords
ii. Require periodic password changes
iii. Require a change of initial or "first-time" passwords
iv. Always verify a user's identity before resetting a password
v. Never ask for a user's password
vi. Change default account passwords
vii. Implement strict controls for system-level and shared service account passwords
viii. Do not use the same password for multiple administrator accounts
ix. Do not allow passwords to be transmitted in plain-text
x. Do not store passwords in easily reversible form
xi. Implement automated notification of a password change or reset

10.6 Annex 6: ICT Asset and Inventory Management Template

Item Description			Location		Purchase Information			Condition and Value		Item Details	
S/N	Description	Category	Dept./Unit	Room	Date	Supplier	Warranty Expiration	Condition	Value	Model No.	Serial No.
1	Laptop	Computer Hardware	ICT	10	10-Jul-2015	Simply computers	10-Jul-2016	Functional	2,700,000	Latitude E54110	271768495