UNITED REPUBLIC OF TANZANIA

MINISTRY OF FINANCE AND PLANNING (MOFP)

ICT Security Policy

February, 2020

Ministry of Finance and Planning

APPROVAL	Name	Job Title/Role	Signature	Date
Approved by	**Doto M. James**	Permanent Secretary		**20th April, 2020**

THE UNITED REPUBLIC OF TANZANIA	
Applicable Public Institution	Title: **MOFP ICT Security Policy** Document No.: **ICTU/002**

TABLE OF CONTENTS

FOREWORD

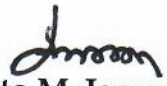
Globally, there has been advancement in ICT and Communications Technologies (ICT) since the end of the 20th Century which led to multiple convergences of contents, computing, telecommunications and broadcasting. Internet represents growth of global computer network which has increased capacity of ICT. As a result, it has impacted the way business is conducted, facilitated learning and knowledge sharing, generated ICT flows and empowered communities in ways that have redefined governance. This transformation is significant to wealth and economic growth.

The National ICT Policy recognized the use of ICT to improve delivery of public services, as a result, in 2004 the Government through Cabinet directed the President's Office Public Service Management (PO-PSM) to start implementing ICT in Government service delivery (e-Government). In April, 2012 PO-PSM established the e-Government Agency (eGA) that was officially inaugurated in July, 2012 with the mandate for coordination, oversight and promotion of e-Government initiatives and enforcement of e-Government standards in the Public Service. In order to have a uniform approach in implementing e-Government, the Government through eGA issued guidelines which directed public institutions to develop their ICT policy.

In compliance with the guidelines, the Ministry of Finance and Planning (MoFP) has developed ICT Security policy which will safeguard and facilitate the efficient and effective use of ICT resources in the Ministry. This will contribute to the achievement of the Ministry's business objectives in the use of technologies as well as safeguarding the Ministry's ICT assets, ICT investments and operations.

Development of this policy has been a collaborative effort. The Policy has been developed in collaboration with the Ministry Management, its staff, consultant from e-Government, and other key stakeholders from Bank of Tanzania, President's Office –Public Service Management, Uongozi Institute, Tanzania Revenue Authority, and Ministry of Works,

Transport and Communication (Communication Sector). I wish to express my appreciation to all of them for their valuable time and effort that contributed to a successful completion of this Policy.



Doto M. James

PERMANENT SECRETARY – TREASURY

1.0 INTRODUCTION AND GENERAL OVERVIEW

1.1 Introduction

MoFP Information and Communication Technology assets are highly valuable and must be closely safeguarded. The Ministry operates within an increasingly electronic, interconnected, and regulated environment that necessitates a consistent and standardized approach to secure technologies and ICT assets. The ICT Security Policy sets out the basis for MoFP in protecting the confidentiality, integrity, and availability of its data, for classifying and handling confidential ICT, and for dealing with breaches of this Policy.

To ensure the continued protection of corporate ICT and to maintain a secure environment, the management team of MoFP strongly believes that an ICT security approach aligned with industry standards is necessary for implementation of its business strategy.

The structure of this ICT Security Policy follows that of ISO/IEC 27001 and 27002 to provide for easy correlation between the standard's requirements and associated MoFP policy statements and its working environment.

1.2 Rationale

It is the mandate of Ministry of Finance and Planning through the ICT unit to ensure ICT assets are protected from all types of threat, whether internal or external, deliberate or accidental in order to maintain, Confidentiality, Integrity and Availability.

The implementation and utilization of ICT Security Policy will ensure efficiency and effectiveness of internal and external operations of the organization as well as improving service delivery and provide secured environment for interactions with private and public institutions.

1.3 Policy Objective

To provide the direction and commitment to deal with ICT Security issues on protecting ICT assets from loss or misuse and ensure integrity, confidentiality and availability of MoFP data.

1.4 Scope of the Policy

This policy is applicable to all users (internal and external), employees, staffs, vendors and any other stakeholder of MoFP infrastructure and information systems. It covers all the ICT assets include physical and logical computing devices either owned, leased or used by MoFP staffs and electronic information held on those assets.

1.5 Purpose

This ICT Security Policy is the basis of Ministry's ICT security program, aimed at Identifying the rules and procedures for all individuals or else accessing and using an organization's ICT assets.

This fact places a significant burden on the MoFP regarding the management and use of its extensive ICT systems resources according to industry standards and best practices. Therefore, the ICT Security Policy aimed at ensuring;

i. Confidentiality, availability, and integrity of electronic ICT captured, transmitted /processed and stored in the MoFP ICT systems and network
ii. Compliance to statutory regulations specifies appropriate practices and defines custodial responsibility for records associated with the MoFP operations.
iii. To streamline the efforts, define and establish areas of priority towards a proper investment into the ICT Security.
iv. Sets responsibility and accountability on the development, investment and management of ICT systems and human resources.
v. The employees and staffs of MoFP are aware of the recommended ICT Security practices and standards.

vi. That the business associated risks are well known by everyone and that the mitigation measures are planned and executed in advance to avoid possible loss and damage ICT assets.

2.0 ICT SECURITY POLICY STATEMENT

The policy statements are intended to help on the best use of the ICT resources at your disposal, while minimizing the cyber security risks. You should understand the following:

i. You are individually responsible and accountable for protecting the equipment, software and information in your hands. Security is everyone's responsibility.
ii. Identify which data is non-public, which includes MoFP confidential data, client data and personal data. If you do not know or not sure ask.
iii. Use the resources at your disposal only for the benefit of MoFP.
iv. Only store MoFP data on encrypted devices.
v. Do not bypass established network and internet access connection rules.
vi. Do not bypass or uninstall your virus checking or firewall software.
vii. Make sure to check against viruses from USB drives and other media brought in.
viii. Do not change or install any unauthorized software or browser 'plug-ins'.
ix. Do not copy or store MoFP data on external devices or unauthorized external locations.
x. Contact Security Administrator for the best solution for secured file transfer.
xi. Report any potential or actual Security Incident to ICT Unit.

2.1 Data and Information Management

To ensure the data protection standards are met, MoFP takes the protection of data and the security measures seriously.

Statements.

i. All user of information system should save their work on the systems and backup potential data to the server regularly.
ii. All system users should be created in MoFP domain for secure access of data.

iii. All confidential or secret data should be encrypted and user is responsible with accountability in any event of loss of data.

iv. Files should only be copied to removable storage when necessary and the storage should be encrypted;

v. Logout your computer when is not in use.

2.2 Human Resource

Employees and staffs are changing positions, job descriptions, either new staffs are joining the Ministry or sometimes some are leaving the Ministry; that set the task of managing the system access privileges for human resource a very challenging issue especially when it comes to the security of information systems on which they had access on.

Statements.

i. When employees are suspended, terminated or resign from service, their systems and network access privileges must be disabled or removed immediately.

ii. When an employee is transferred to another duty station or is assigned a different job role, department of human resource shall communicate to the ICT Unit.

iii. Upon recruitment, staff shall be provided with this policy as part of an induction package for reading and understanding.

iv. ICT Security Policy awareness should be planned and conducted regularly to employees.

2.3 Asset Management

MoFP has the responsibility to properly acquire, use and dispose the ICT assets. Therefore, MoFP shall adopt the best standards and procedures in disposing them without jeopardizing the integrity, availability and confidentiality of the information it processes or store.

Statements.

MoFP shall ensure;

i. ICT Unit shall coordinate acquiring of all ICT assets from manufacturer approved vendors

ii. Only approved software configurations should be applied to new hardware

iii. Unauthorized changes or re-configurations of standard ICT components are not allowed.

iv. Users should take appropriate care with any hardware that has been issued to them and lost/Stolen hardware should be reported immediately

v. The inventory of ICT assets (register) is created and updated every time an asset disposed or acquired.

vi. Before disposing any of the digital equipment such as desktop computer, laptop, scanner, printer, server and any other electronic or computing device, all data stored must be permanently deleted.

vii. The ICT unit in collaboration with GAMD shall consolidate a list of all ICT assets eligible for disposal.

2.4 Password Management

To make information secure, password management is a critical issue in maintaining confidentiality of data.

Statements.

i. Do not use dictionary words - All real words are easy to guess.

ii. Use acronyms relevant to you only, mnemonics, random letters, etc., and insert non-alphabetic characters in the middle of the word.

iii. Use a mixture of UPPER and lower case, numbers and special characters or long phrases that only you can remember.

iv. Password must be changed regularly;

v. Do not provide your password to any unknown website, email or phone calls to avoid hackers.

2.5 Electronic Mail Management

E-mail is a business communication tool which all MoFP employees are requested to use in a responsible, effective and mandatory.

Statements.

i. When emailing sensitive files externally the files should be password protected /encrypted

ii. Check email addresses prior to sending any files

iii. All official communications should use Ministry's e-mail system (hazina.go.tz).

iv. Do not open e-mail from unknown sender to avoid spams.

v. Logout your mail system when is not in use.

2.6 Internet Access

MoFP provides Internet access to all staff to assist them in carrying out their duties such as looking up details about suppliers, products, accessing governmental information and other work-related information.

Statements:

i. There shall be a firewall to filter data traffic coming into MoFP's network through its internet access connection.

ii. Internet access shall be provided to users to support MoFP daily activities

iii. Users shall not use the Internet to transmit any proprietary, confidential, or otherwise sensitive information without the proper controls.

iv. Users shall not use MoFP internet for their personal use.

v. All information/data posted to the Intranet should be checked for virus/bugs.

vi. Internet usage activities of MoFP staff may be monitored by the ICT team.

vii. Users are not allowed to connect any personal devices on MoFP Network to access the Internet directly without permission from ICT Unit.

2.7 Remote Access and Electronic Communication

For MoFP staff to achieve access to the centralized services at the head office servers; there is supposed to be a secure and reliable channel to and from remote Office.

Statements:

i. User shall obtain proper authorization from ICT unit for allowing remote access working.
ii. Avoid using remote access working from public systems, such as internet cafes.
iii. For remote access to the MoFP ICT Infrastructure resources only the officially supported and approved facilities by the internal ICT Unit are to be used.
iv. The associated security policies must be applied for any remote connection.
v. Online Communication from/within MoFP Offices to an external party may only use MoFP approved communication channels.
vi. Personal internet connections or connectivity devices are strictly prohibited.

2.8 Network Management

At MoFP we more than 30 regional sub offices that form part of our whole network, a secure network is critical to the security of our business:

Statement:

i. External facing networks should be firewalled to an appropriate level
ii. Physical and logical network changes should only be made by approved users.
iii. Networks should be segregated on a geographical and/ or business line basis
iv. Appropriate controls should be in place at network interfaces
v. WAN services should only be acquired through approved vendors
vi. Network event logging and monitoring should be implemented
vii. All network equipment should use licensed software.

2.9 Wireless Networks

Wireless technology is inherently insecure. The ability to access the business network resources without being physically connected to the cable network means that the security threat by the wireless access is much higher than those posed by the cable connection.

Statements:

i. Only approved wireless access points should be used or accessed.
ii. Wireless networks should always be encrypted.

iii. Wireless internet connections to employees' personal devices will be done by ICT officer.

iv. Office guests will not be allowed to connect to office wireless internet (Wi-Fi) services unless with approval from Head of ICT

v. Passwords to connect to Office wireless internet services will be frequently changed to avoid non-office members to use or compromising the services.

2.10 Workstation Security

These devices are essential tools that can be used by a member of staff or employees to complete different tasks and assignments (Users' Computer).

Statements

i. All workstations should have corporate-approved anti- virus software installed and enabled

ii. All workstations should have password protection

iii. All workstation should be installed with genuine software

iv. Do not allow unauthorized users to access your workstation

v. Take appropriate steps to maintain the physical security of your workstation

vi. Logoff your workstation when is not in use.

2.11 Mobile Device

Every mobile device capable of accessing MoFP information shall be configured in line with the requirements described in this policy.

Statements;

i. MoFP's information shall be only processed by registered mobile devices.
ii. Mobile devices used by staffs shall be configured with necessary information security controls by ICT personnel.
iii. All mobile devices shall be installed with up to date software (eg antivirus).
iv. A personal firewall shall be installed to provide protection from unauthorized intrusions.
v. All mobile devices shall have password to protect form unauthorized user.

vi. All mobile devices supplied by the Government or by MoFP remain the property of MoFP.
vii. Employees must immediately inform the ICT unit when mobile device is stolen or lost.
viii. MoFP network and system passwords must not be stored on mobile devices unless it is a system limitation.
ix. Do not connected directly to MoFP Internal network untrusted mobile devices.
x. Mobile devices should only use guest network access while in a MoFP Office.

2.13 Software Developmentand Maintenance

At MoFP we have a high-dependency on in - house software development to conduct our day-to-day business:

Statement.

i. Applications should comply with the Privacy by Design principle
ii. A Privacy Impact Assessment should be completed for major software changes
iii. Security requirements for software should be documented as part of the development process
iv. Software changes should be subject to change control procedures
v. Only authorized users are permitted to deploy software changes

2.14 Licensing

MoFP uses software from a variety of third parties, copyrighted by the software developer and unless expressly authorized to do so.

Statement:

i. Employees do not have the right to make copies of the software.
ii. MoFP should respect and adhere to all computer a software copyrights and terms of all software licenses to which MoFP is a party.
iii. MoFP should manage ICTs software assets and ensure all used software are legal on ICTs workstations and servers.

2.15 Backup

Despite of all protection measures put against threats over information systems; yet

information can be hacked or data can be lost, sometimes the entire systems can be damaged due to various threats that pose in a day to day operation of the information system. To ensure business continuity backups should be done.

Statement:

i. Backup of data and applications shall be done by the designated ICT personnel on all critical information systems on daily basis.

ii. Data backed up from MoFP's information systems shall be moved to offsite location either through tapes, CDs, DVDs, external storage devices or through network

iii. The backup media must be precisely labeled and accurate records must be maintained.

iv. At offsite location, data backup media shall be stored in fire proof cabinets.

v. Back up data shall be regularly tested to ensure integrity and usability of the data

2.16 Malicious Code

Software and information processing facilities are vulnerable to the introduction of malicious codes such as computer viruses, network worms and Trojan horses. It is for this reason that MoFP is required to protect the internal resources and infrastructure from these malicious codes.

Statements:

i. MoFP shall ensure that all servers and workstations are installed with the updated antivirus software.

ii. Users are prohibited from propagating malicious codes.

iii. Users shall immediately stop using the affected computer if suspects virus infection.

iv. Users must not abort automatic antivirus software update and scanning.

2.17 Outsourcing

Due to the limitation of its IT manpower and ICT resources, MoFP may decide to outsource some of its core ICT activities to outside vendors. The outsourced services or access to MoFP's information systems may pose a significant security risk and hence there is a need to manage it.

Statement;

i. Before providing the outsourced company with access into MoFP's information systems, head of ICT shall make sure non-disclosure agreement has been signed.
ii. MoFP shall ensures that the outsourcing procedures are followed before outsourcing.
iii. All ICT outsourcing should get approval from Accounting Officer.

2.18 Business continuity management

MoFP maintains a group Business Continuity Management Policy (BCMP). This requires sub-functions to develop detailed business Continuity plans under ICTs umbrella. The ICT function must ensure that the Business Continuity Plan adequately addresses business Continuity of the ICT environment.

Statements:

i. MoFP should make sure that, Disaster Recovery Plan is in Place and periodically tested.
ii. MoFP should make sure security incident procedure are followed in case of events.
iii. Disaster backups should not be used for operational recovery.

2.19 Physical Security

MoFP ICT security is dependent on the physical security of ICT resources such as built data centers, backup sites and on- premise computer rooms:

Statements:

i. Critical server rooms must be located in a place where the risk of natural disasters is minimized.
ii. All entry points to ICT facilities should be controlled with access control mechanisms.
iii. Appropriate environmental controls such as air conditioning and fire suppression systems should be in place
iv. There must be a clean power backup computer premise.
v. Food and drink is not allowed on- computer premise

3.0 RESPONSIBILITIES

ICT Security is everyone's responsibility, although the ultimate responsibility resides with the MoFP Directors/ Executive Management. This responsibility cascades down through a series of designated roles.

3.1 Head of ICT Unit

The Head of ICT is responsible for:

i. ICT security management within MoFP, acting as a central point of contact on security for both staff and external MoFP's;
ii. Managing and implementing this policy and related policies, standards and guidelines;
iii. Monitoring and responding to potential and/or actual security breaches;
iv. Ensuring that staff are aware of their responsibilities and accountability for information security;
v. Providing specialist advice on security issues;

3.2 Security & Privacy Committee

The Security & Privacy Committee is responsible for ICT risk within MoFP, advising the executive management on the effectiveness of management of security and privacy issues across the Group and advising on compliance within relevant legislation and regulations.

3.3 Directors/ Managers/ Head of Units

These shall be individually responsible for the security of their environments where information is processed or stored. Furthermore, they are responsible with

- Ensuring that all staff, permanent, temporary and/or contractors, are aware of the information security policies, procedures and user obligations applicable to their area of work and of their personal responsibilities for information security;
- Determining the level of access to be granted to specific individuals;
- Ensuring staff have appropriate training for the systems they use;

- Ensuring staff know how to access advice on information security matters.

3.4 All Staff

All staff are responsible for ICT security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action.

In particular, all staff should understand:

i. What information they are using, how ICT should be used, stored and transferred in terms of data security;
ii. What procedures, standards and protocols exist for the sharing of information with other parties;
iii. How to report a suspected breach of information security within the MoFP;
iv. Their responsibility for raising any information security concerns

All MoFP users are responsible with adhering to the provisions of this Policy and all related policies, standards, guidelines and procedures and must report every incident of misuse or abuse of which they become aware as described in the MoFP Security Incident Management Procedure.

3.5 External contractors

All contracts with external contractors that allow access to the MoFP's data or information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external MOFP comply with all appropriate security policies.

4.0 BREACHES

Breach of this Policy will be taken seriously and may result in disciplinary actions in conformity legal and contractual framework, including termination of employment. Any user disregarding the rules set out in this Policy or in applicable laws will be fully liable and MoFP will disassociate itself from the user as far as legally possible.

All breaches of this policy must be reported to the respective Manager/Director for appropriate

action and/or using the process described by the MoFP Security Incident Management Procedure.

5.0 REVISION

This policy will be reviewed after every two (2) or earlier if necessary.

6.0 GROSSARY AND ACRONYMS

6.1 Glossary

ICT Security Policy – A document that elaborate on the Public Institution's ICT Management Philosophy by providing general statements of purpose, direction and required activities for the ICT Security Management Framework, commonly known as ICT Security Policy of an Institution.

LAN – The office network; normally controlled and managed by own domain controller.

ICT Infrastructure – Deployed hardware and software (or applications) that work together to forms the production environment for one's business.

ICT Systems – Applications running on a particular platform to accomplish desired tasks; it normally accepts and process data to give a desired ICT to the user. It consists of hardware and software that works interactively.

Encryption – A process of converting readable message into a form that cannot be understood by third party unless that party has the decryption key (secret code to convert the message back to readable one)

Decryption –The process of turning the cipher text (unreadable message) back to readable text

Primary Site – refers the current production / working environment where users and systems are working to accomplish desired tasks. It includes the ICT systems and associated network.

Recovery Site – The failover environment that would be called on duty upon demand especially when the primary site is down and unable to perform. It is sometimes referred to as "Disaster recovery site "

Firewalls – Tools to protect the backside (inside) network resources from outside. They normally exposed to the internet to shield the inside part from the internet incoming threats. There are hardware and software-based type of firewalls.

Data Centre – Refers to the collection of corporate servers, network and communication equipment's. They are normally located to a closed protected room

VoIP – A telephone services provided over the internet as the means of transmission.

Broadband - Is the high-speed transmission (wide bandwidth) of various types of signals and traffics over the medium like fiber optic.

Bandwidth – Is the data transfer rate. The logical value of data / signal transmission; the bigger the value the high rate of transmission; sometimes referred to as the channel capacity for data transfer

Internet – Is the global system of interconnected computer networks that use the standard internet protocol suite to connect billions of users worldwide.

Virtual Private Network – An established private communication channels that normally span through the internet the private channels are protected from the unauthorized access from internet.

E-environment – An office or working place where lot of its business operations are automated by use of computer applications.

Split-Tunnelling – A type of computer networking which allows a VPN user to connect to internet (a public network) and a local LAN or WAN at the same time using the same physical network connection

Penetration Test (Pen Test) – Is a method of assessing security of a network or computer system by simulating an attack from malicious outsiders who don't have authorized access to the organizations business network. The aim is to analyse the points of vulnerabilities (weaknesses) so that can be addressed and fixed.

World Wide Web (www) – Is a system of interlinked hypertext documents accessed via the internet.

6.2 LIST OF ACRONYMS

ICT – Information and Communication Technology

VoIP – Voice over Internet Protocol

USB – Universal Serial Bus

LAN – Local Area Network

VPN – Virtual Private Network

WAN – Wide Area Network

MOFP – Ministry of Finance and Planning

SPOC – Single Point of Contact

GAMD – Government Asset Management Division