THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF FINANCE

ICT SECURITY GUIDELINES

DECEMBER, 2012

PERMANENT SECRETARY,
MINISTRY OF FINANCE,
P.O BOX 9111,
DAR ES SALAAM.

FOREWORD

The Information and Communication Technology (ICT) development and its wide utilization across the world have made ICT to be used as strategic tool to achieve social economic development goals globally. Increasing capacity of ICT has further been empowered by the growth of a global network of computer networks i.e. the Internet. It has impacted the way business is conducted, facilitated learning and knowledge sharing, generated global information flows, empowered citizens and communities in ways that have redefined governance, and has created significant wealth and economic growth and hence resulting in a global information society.

By recognizing the impact of ICT in achieving ministerial objectives, the Ministry of Finance (MoF) has deployed several ICT systems for effective and efficient service delivery. Some of these systems can only be accessed internally while others outside the Ministry. The Ministry further understands that ICT systems are vulnerable to attacks and there are security threats which need mechanisms to protect organizational ICT resources against the threats and attacks. In addition, improper handling (collection, storage, processing and transmission) of organizational data would infringe rules and regulations governing data confidentiality, integrity and availability. Moreover, the Ministry had formulated the Ministerial ICT Steering Committee in the year 2010 to oversee proper utilization of ICT resources in the Ministry as well as monitor all ICT activities while ensuring that they are conducted according to the best practices.

Thus, this Guide provides mechanisms for securing information systems assets (personnel, data, hardware, software and communication channels). In addition, it provides guidance on how to handle third party access to organizational resources without compromising organizational security.

Further, MoF ICT Security guidelines are intended to harmonize the idea put forward in the two drafted ICT policy documents namely the MoF IT Policy Draft 'developed in 2006 by Financial Information Systems Management

Department as well as the Integrated Financial Management Systems Network Security Policy Version 1 developed by the Accountant General's Department. The Guidelines put forward best practice when using the Ministry of Finance computing resources. These Guidelines are in line with the National ICT Policy 2003, National Security Act 1970, Government Circular Number 1 of 2011 of Chief Secretary, and other relevant Government circulars that aim at creating a secured environment that would enhance service delivery while protecting organizational resources.

It should be clear that, in a scenario where an employee or non-employee fails to comply with these Guidelines; Disciplinary measures will be taken against him/her as per Public Service Acts, Regulations, Circulars and other Government Directives.

PERMANENT SECRETARY – TREASURY/MINISTRY OF FINANCE

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AMP	–	Aid Management Platform
BCP	–	Business Continuity Plan
CCTV	–	Closed Circuit Television System
CD	–	Compact Disk
CS-DRMS	–	Commonwealth Secretariat - Debt Recording and Management System
DAHRM	–	Director of Administration and Human Resource Management
DHCP	–	Dynamic Host Configuration Protocol
DMZ	–	Demilitarized Zone
DNS	–	Domain Name System/Domain Name Service
DoS	–	Denial-of-Service
DRS	–	Disaster Recovery Site
DVD	–	Digital Versatile/Video Disc
GoT	–	Government of Tanzania
ICT	–	Information and Communication Technology
IDS	–	Intrusion Detection Systems
IFMS	–	Integrated Financial Management System
IP	–	Internet Protocol
IPX	–	Internet Protocol Exchange
IPS	–	Intrusion Prevention Systems
ISP	–	Internet Service Provider
LGAs	–	Local Government Authorities
MAC	–	Media Access Control
MDAs	–	Ministries, Independent Departments and Agencies
MoF	–	Ministry of Finance
NIDS	–	Network Intrusion Detection Systems
NIPS	–	Network Intrusion Protection Systems
PC	–	Personal Computer
PCMCIA	–	Personal Computer Memory Card International Association

PDA	–	Personal Digital Assistant
PO-PSM	–	President's Office - Public Service Management
VPN	–	Virtual Private Network
SBAS	–	Strategic Budget Allocation System
SLA	–	Service level Agreement
SSID	–	Service Set Identifier
RFC	–	Request for Comments
TCRA	–	Tanzania Communications Regulatory Authority
TLS/SSL	–	Transport Layer Security/Secure Socket Layer
UPS	–	Uninterruptible Power Supply
User ID	–	User Identification
HR	–	Human Resource

DEFINITION OF TERMS

Cloud computing - is a technology that uses the internet and central remote servers to maintain data and applications.

Computer viruses - is a relatively small software program that is attached to another larger program for the purpose of gaining access to information or to corrupt information within a computer system.

Cryptography - The art of protecting information by transforming it (*encrypting* it) into an unreadable format called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text.

Cyber attack - is a term for any illegal activity that uses a computer as its primary means of commission.

Data availability - refers to how available data is when stored in some form, usually in reference to remote storage of data through a network or external storage media.

Data confidentiality - means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Data integrity - is a term used to refer to the accuracy and reliability of data.

Encryption- is the conversion of data into a form, that cannot be easily understood by unauthorized people unless to the intended recipient with a proper coding key.

End user- is the person that a software program or hardware device is designed for.

ICT unit – is defined in this document as the unit that coordinates and manages ICT services in the Ministry.

Malicious code - refers to a broad category of software threats that can cause damages or undesirable effect to computers or networks.

MoF disclaimer - A statement intended to specify or delimit the scope of rights and obligations that may be exercised and enforced by parties in a legally recognized relationship.

Phishing attack - The act of sending email to a user falsely claims to be an established legitimate enterprise in an attempt to steal users' private information that will be used for theft.

Spam - is unsolicited commercial advertisements distributed online. Electronic junk mail or junk newsgroup postings.

Temporary employee – is an employee who works for only a limited period of time.

Insider threat – is a malicious hacker who is the current or former employee, contractor, business partner of the institution obtains access to the computer systems or networks and then conducts activities intended to cause harm to the institution.

System abuse – can be defined as using the rules and procedures meant to protect a system in order, instead, to manipulate the system for a desired outcome.

Access Protocol – A protocol used between an external subscriber and a switch within a network.

1. INTRODUCTION

1.1. Background

Due to the benefits brought by ICT to the modern functioning of the Government, Ministry of Finance has been using ICT to deliver services to the public since 1965 ranging from revenue collection and external resources management. Other activities which follow the same suite are planning, budget formulation and preparation of payroll and pension management to name the few.

The Ministry has invested in the development of shared ICT infrastructure consisting of structured wired and wireless technologies to most of its buildings located at the head office and remote offices including other organizations. Also, the Ministry has invested on various software technologies such as IFMS (Epicor), Payroll system, CS-DRMS, AMP and SBAS. Others include software for office application, communication and collaboration.

The Ministry's commitment to use ICT to improve service delivery to the public faces many security challenges brought by the technology advancement. To address information security issues, the Ministry of Finance has developed two documents, the first versions of IT Policy and IFMS Network Security Policy. Furthermore, MoF has been implementing Circulars and Regulations issued by the Government of Tanzania on proper use of ICT facilities and confidentiality of data, including Circular No. 5 and No. 6 of 2009 issued by the Permanent Secretary, President's Office – Public Service Management (PO-PSM).

As ICT systems continue to be deployed, it is imperative that necessary policies, guidelines and operational procedures be put in place to ensure their proper usage, management, administration and security. In addition, the increasingly rapid evolution and growth in the complexity of new systems and networks, coupled with the sophistication of changing threats and the

presence of intrinsic vulnerabilities, present demanding challenges for maintaining the security of ICT systems and networks. In response to these challenges, formulation of Information Security Guidelines is essential to ensure adequate levels of security to facilitate proper use of ICT facilities, as well as compliance with pertinent circulars and regulations governing the use of ICT facilities.

1.2. Purpose

The main purpose of these Guidelines is to provide framework for selecting, implementing, and managing ICT security services by guiding the organization on how to manage ICT assets. Moreover, the Guide intends to protect both the data stored and processed within MoF computer systems together with the services provided by these systems for the purpose of protecting information confidentiality, integrity and availability.

In addition, the Guide aims at creating a unified environment of handling ICT security issues for all MoF staff and people who access MoF's information systems resources. It also guides on issues to consider while developing agreements that define the service levels for service providers. Furthermore, the Guide provides information for decision makers and other relevant parties on security issues for the purpose of obtaining comprehensive ICT security services.

Therefore, this document is meant to translate National ICT Policy 2003, Public Service Act 2002 and existing circulars into implementation in the form of guidelines which are easy to follow on the day to day operations.

1.3. Scope

This Guide applies to all MoF employees, including all officers, support staff, temporary staff, partner agency staff, contractors and all users from MDA's/LGA's using MoF computer services (e.g IFMS). All staffs are required to adhere to these Guidelines to ensure that desired level of ICT security is achieved and maintained.

This document addresses security considerations in the following major areas:

i. Physical and environmental working areas.
ii. ICT resource access control
iii. Data and information security
iv. Network and its services (e.g. e-mail)
v. Software deployment and use
vi. Business continuity management
vii. Third party management
viii. Training, awareness and support
ix. Hardware retention and disposal
x. Personnel security
xi. Monitoring and evaluation

The Guide will be reviewed from time to time and when the need arises in order to address new technological challenges and new business practices.

1.4. Disclaimer

This document is expected to provide guidance on the proper use of ICT facilities in MoF, it is not by any way exhaustive and the proper use of ICT facilities is not limited to what is documented here in.

2. PHYSICAL AND ENVIRONMENTAL SECURITY

Physical and Environmental security aims at protecting MoF's ICT facilities i.e. Hardware, software, data and communication infrastructure from

unauthorized access, hazards, intentional or unintentional damage, as well as theft. Breach of physical and environmental security may lead to loss of confidentiality, integrity, and availability of information systems assets. To prevent such loss, measures such as adequate air conditioning, fire detection and suppression systems, reliable power supplies, controlling physical access and suitable emergency preparedness should be in place. The envisaged measures are as follows:

2.1 Measures against Fire

i. Rooms that host servers should be non-smoking zones, fireproof, fitted with smoke detectors and have automatic or portable fire extinguisher systems.
ii. Smoke detectors and fire extinguishers should be regularly tested to ensure that they are in good order and all tests have to be documented.
iii. Materials which can easily catch fire should be disposed of and those documents which are still in use should be stored in a secure place.
iv. Activities such as rewiring, welding or cutting, undertaken as part of structural changes to the premises, should be monitored by ICT staff, so long as there is proof of safety of new wiring required.
v. Clear fire instructions should be available and in the event of fire, these instructions should be followed.
vi. Regular fire practices (fire drills) should be conducted frequently.

The head of administration and human resource department in collaboration with the ICT unit will ensure the implementation of the above measures.

2.2 Measures against Floods

i. Servers should be well mounted on racks and other equipment should be kept off the ground, placed on tables or desks.
ii. Clear flood instructions should be available and in the event of flood,

these instructions should be followed.

iii. All water tanks and plumbing at MoF premises should be inspected regularly to prevent leaks and overflow of water. All inspection reports should be well kept for future reference.

The head of administration and human resource department in collaboration with the ICT unit will ensure the implementation of the above measures.

2.3 Air Conditioning

i. The Server rooms and computer rooms should be adequately air conditioned to provide conducive environment for the ICT equipment.
ii. The air conditioners should be serviced regularly to ensure continuous performance.
iii. Air conditioning failure should be reported for immediate remedial measures.

The head of the ICT unit will be responsible for the air conditioning measures.

2.4 Power Outage

To ensure ICT services availability, alternative power sources such as Uninterruptible Power Supplies (UPS) and generators should be used to provide continuous power supply based on the following requirements:

i. UPS should be installed as appropriate to all ICT facilities.
ii. Specialized UPS of appropriate capacity should be installed in all server rooms.
iii. Non-critical electrical equipment, especially high power consumption equipment such as photocopiers, printers and kettles should not be connected to UPS sockets.
iv. A generator of appropriate capacity should be serviceable at all times as backup power supply in the event of power outage.

The head of administration and human resource department in collaboration

with the ICT unit will be responsible for ensuring power supply.

2.5 Measures against Theft

i. Non-MoF employees should not use MoF ICT resources without prior relevant written authority.
ii. Internal movement of ICT equipment owned by MoF should be authorized by the relevant authority in written form. Proper record should be kept for such movements.
iii. Moving ICT equipment owned/leased by MoF outside the premises should follow laid down procedures.
iv. Appropriate locks on windows and doors should be maintained. Doors should be kept locked when rooms are not in use. Secure system for keys and combinations should be maintained. In the event of security breach, compromised lock should be changed.
v. Alternative physical security strategies should be used when appropriate.
vi. All legitimate visitors should be logged at the entrance to MoF building and must declare ICT equipment.
vii. All staff must declare personal ICT equipment at the entrance.

The head of administration and human resource department will ensure the implementation of the above measures.

Note:

To avoid ICT equipment and information loss, it is prohibited to bring personal ICT equipment within MoF premises unless permission from the authority is granted.

3. ACCESS CONTROL

Access control includes measures that need to be taken to control user access to computing areas and their associated systems. This is categorized into two areas namely physical access and logical access.

3.1 Physical Access Control

Both Server and Computer rooms should be protected against unauthorized access. The authorization of access to Computer and Server Rooms, and Disaster Recovery Site should base on the following requirements:

i. Normal hours of entry for the Computer and Server Rooms will be limited to approved times.
ii. Staff/Visitors authorized to enter the Server and Computer rooms should be accompanied by designated officer. Visitors should be logged in the register book.
iii. All staff should be trained on how to observe access procedures.
iv. Visitors should display visitors pass at all times.
v. ID cards and keys should not be shared or exchanged.
vi. All staff who have their access rights withdrawn should return the ID cards to Permanent Secretary-Treasury/MoF.

3.2 Logical Access Control

3.2.1. Managing User Profiles

Access to the Computer systems should be authorized by the relevant authority, or appropriate delegated officer. Access to any particular data file should be based on the user's roles as established by his or her official duties, and should be reflected in the provision of specific authorization codes, passwords or other access-enabling means.

i. Users should be issued Unique User IDs that are produced following a

standard naming convention.

ii. Before being granted logical access, users should complete a “User Access Permission Application Form” that defines access privileges. The user permission application form is attached as appendix A.

iii. Users should be granted access and privileges based on their roles.

iv. Changes to Access Rights should only be made under authorization of the relevant authority.

v. Designated Systems administrator should review and maintain User Access Profiles.

vi. Privileges should be allocated to network and/or application software accounts on an 'as needs' basis. i.e. no more access should be offered than is necessary to carry out the user’s needs.

vii. User account names should not indicate their associated privileges.

viii. The default password for an account should be constructed in accordance with systems password policy.

ix. Working groups or teams should be assigned their own access profile with specific network resource access. Individual users allocated to such groups should be given an account linked to that access profile.

3.2.2. Managing Network Access Controls

i. Access to resources on the systems network should be restricted unless specifically authorized.

ii. Users are expressly forbidden from making unauthorized alterations or extensions to the network.

iii. A register of network devices, their access restrictions and the protocols in use should be kept by the Network Administrator.

iv. All changes to network configurations should be recorded in the register, along with authorization for the changes.

v. Users should be permitted to use only those network addresses issued to them by the relevant authority.

vi. Virtual networks should be set up for specific groups of users. These

groups should have Group User Access Profiles, on which the user access profiles of individual team members should be based.

vii. Users inside MoF network should not be allowed to use devices which connect to external networks, for example, the use of modem to connect to the internet.

viii. Remote MoF users should connect to servers using a secure communication channel such as Virtual Private Network on dedicated communications lines with end-to-end encryption.

ix. Network devices and traffic should be monitored regularly.

x. Results/Logs from the firewall should be reviewed by ICT security officer to confirm there have been no unexpected attempts to connect.

xi. Users should not extend or re-transmit network services and traffic in any way i.e. they should not install a router, switch, hub, or wireless access point to the systems network without being approved.

xii. Users should not install network hardware or software that provides network services without being approved.

xiii. Computers that require network connectivity should conform to systems standards.

xiv. Users with administrative privilege should not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, system users should not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the system network infrastructure.

xv. Users are not permitted to alter network hardware in any way.

3.2.3. Controlling Administrative Access or Special Access

Employees with administrative access or special access privileges to the system are subject to additional controls for creation, use, monitoring and removal of their user access profiles based on the following requirements:

i. MDAs, LGAs and Regional Sub-Treasuries should submit to a relevant

Authority a list of administrative contacts for their systems that are connected to the MoF systems network.

ii. All users of administrative or special access accounts are given account management instructions, documentation, training, and authorization and should meet the Systems Password Policy.

3.2.4. Passwords Management

The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords should not be shared with any other person for any reason.

i. Passwords should be chosen by the user not by the systems administrator. Where this is not practical, the password should be generated and the user should be forced to change the password at first logon.

ii. Users should sign "User Access Permission Application Form" that a password has been received, that it will be kept secret, and changed frequently.

iii. Disclosure of passwords is prohibited.

iv. Paper based records of passwords of systems super user should be placed in a sealed envelope, signed by two authorized persons across the seal, and keep it in a locked, fireproof safe.

v. Passwords should be changed the moment that a breach of confidentiality is suspected.

3.2.5. Controlling Remote User Access

Remote access control procedures should provide adequate safeguards through robust identification, authentication and encryption techniques based on the following requirements.

i. If an authorized user fails to gain access through the secure

communication channel such as VPN, this should be immediately reported to the ICT unit for investigation.

ii. Remote User accessing MoF systems should be authenticated by remote access server.

3.2.6. Clear Screen

All users of workstations, PCs and laptops with access to system, or containing related files, should ensure that their screens are clear of data when not in use. Moreover, user computers should be set so that they automatically switch to a standby mode after a period of inactivity. A password should be needed to regain access to the screen.

3.2.7. Logon and Logoff from Computer

To avoid Information security breaches, users should lock or log off their computers while they are not in use. If a user is unable to log on, it might indicate that someone has achieved unauthorized access using that user's name and password. Where the 'User Logon Register' or operator/administrator logs show incorrect or unusual entries, it could indicate that data has been accessed and therefore possibly lost or stolen. The following requirements should be adhered to:

i. Every user should ensure that their user name and password are kept secret.

ii. If users are unable to logon to the system and denied service, they should double-check that the user name and password are correct and ensure that they are not still logged on elsewhere on the system.

iii. If users are still unable to log on, they should immediately inform their systems administrator. They should not ask to 'borrow' the user name and password of another user in order to log on.

iv. Users should 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.

v. Designated Systems Administrator should monitor the 'User Logon Register' or operator/administrator logs for unusual entries.
vi. Designated Systems Administrator should disable any suspicious logon.
vii. Designated Systems Administrator should report inability of users to log on to the designated Information Security Officer.
viii. Designated Systems Administrator should double check that users have logged off at the end of the working day.
ix. Users should ensure that they log off computer workstation before leaving their desk.

ICT unit will be responsible for both physical and logical access control measures.

4. DATA AND INFORMATION SECURITY

Data security is a critical responsibility for every institution. Every piece of data can be of value to fraudsters as they can access multiple sources of information and aggregate it. It is therefore, necessary that, MoF data and information is protected from unauthorized access, loss, misuse, destruction and falsification.

This section provides guidelines pertaining to data and information handling that includes data collection, storage, processing and transmission as stipulated in the Government Circular number 5.

4.1 Data Collection, Entry and Processing

All processes of data collection, data entry and processing should be done in such a way that the records collected and captured are correct and complete. Data captured should then be validated for accuracy by relevant departments/units.

4.1.1 Data Storage

i. All users of information systems should save their work on the system regularly.
ii. When information and data is stored on local disks (e.g. notebook computers), they should be backed up to the server regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

4.1.2 Data Access

i. Authentication and authorization functions should be used for all users of MoF electronic data and information resources.
ii. Procedures to manage access, authentication and authorization should be developed to support and manage these activities. Such processes

and procedures should include but not limited to user passwords for network and application access, biometric access mechanism, tokens and electronic key devices.

iii. All system users should be created in a central authentication database.

iv. All information within MoF should be classified according to government classification as stipulated in Records & Archives Management. Act. No. 3 of 2002.

4.2 Transfer and Exchange of Information

Data or information may only be transferred across networks or copied to other media when the confidentiality and integrity of the data is reasonably assured. The security mechanisms should reflect the sensitivity of the information involved and the following security conditions should be observed.

i. Information classified as confidential or secret should be encrypted.
ii. Private encryption keys should be physically exchanged rather than transferred electronically.
iii. Management responsibilities for controlling and notifying transmission dispatch and receipt.
iv. Minimum technical standards for packaging and transmission.
v. Use of reliable and trusted courier for data transportation/transfer.
vi. Responsibilities and liabilities in the event of loss of data.
vii. Use of an agreed labeling system for critical information.
viii. Technical standards for recording and reading information and software.

4.3 Security of Media in Transit

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. Thus, it is important to safeguard computer media

being transported between sites based on the following requirements:

i. Reliable and trusted transport or couriers should be used.
ii. Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.
iii. Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification e.g. by use of locked containers, delivery by hand, or use of tamper-evident packaging.

Head of the ICT unit will be responsible for security of media in transit.

4.4 Data Retention and Disposal

i. MoF should ensure that information is retained for appropriate time frame depending on requirements as in Records & Archives Management. Act. No. 3 of 2002.
ii. All data to be disposed off should be erased permanently from any storage media. Data storage media should be verified that data is erased and cannot be read before disposing them as stipulated in Records & Archives Management. Act. No. 3 of 2002.

The head of the ICT unit will be responsible for data retention and disposal.

4.5 Using Live Data for Testing

The use of live data for testing new systems or system changes is only permitted where adequate controls for the security of the data are in place. Using live data for testing can severely compromise its integrity and confidentiality and should base on the following requirements:

i. Where contracted suppliers and other third party staff are involved, a non-disclosure agreement should be signed, together with a

declaration of compliance with MoF ICT Security Guidelines.

ii. Designated system developers should not be permitted to access the live system and its database.

iii. Safe and secure copy of the data should be provided, once the terms of use have been authorized.

iv. Development and testing work should be isolated from normal processing work by means of separate machines or partitions.

v. The techniques used to capture the live data should not permit subsequent or additional access to the live system by the Designated System Developers.

vi. Output from testing should be differentiated from live output (e.g. by different colored paper or overprinting the words 'Test Data'). All test output should be kept within the test room/area.

vii. Test files that contain copies of live data should be disposed of after use. Test printouts containing live data should be destroyed after use.

The head of the ICT unit will be responsible to ensure that the above guidelines are adhered to.

5. NETWORK, INTERNET AND E-MAIL SECURITY

With networked or distributed applications, the security of multiple systems as well as the security of the interconnecting network, internet and its services is important, especially when public access wide area networks are used. This is due to the fact that while internet is increasingly becoming a standard working tool for organizations, criminals may target system via the internet. This could result in serious loss of confidential information or serious damage to information systems, such as premeditated virus attacks. To protect against premeditated or opportunistic attacks, security on the network is to be maintained at the highest level consistent with user needs.

5.1 Network Security

The designated MoF network administrator should ensure the security of information in networks and protection of supporting infrastructure based on the following requirements:

i. Keep network secured by minimizing number of network interface points between "secured" network and "non-secured" network.
ii. Keep network secured by separating internal networks and external networks.
iii. MoF networks should not be extended to other external networks without permission.
iv. Only allow authorized traffic to enter the "secured" network.
v. Use multiple mechanisms to authenticate user (e.g. password system plus preregistered IP/IPX network plus pre-registered MAC address/terminal number).
vi. Manage the network with network management system.
vii. Encrypt data with approved encryption algorithm before transmitting over the network.
viii. Firewall, and intrusion prevention and detection system should be installed and properly configure to protect MoF network.

ix. All access points of the network layout should be identified, and checks carried out to verify that safeguards are operational.

The head of the ICT unit will be responsible to ensure the guidelines for network security are adhered to.

5.2 Wireless Network Security

Wireless Network is a type of network that uses high-frequency radio waves. With the advancement of technology and advances in price/performance, wireless accessibility is becoming increasingly deployed in the office or in public places. Security controls should base on following requirements:

5.2.1 Management Controls

i. Wireless network should be used with sufficient authentication and transmission encryption measures in place, complemented by proper security management processes and practices.
ii. Designated System Administrator should develop a coverage map of the wireless network, including locations of respective access points and Service Set Identifier (SSID) information so as to avoid excessive coverage by the wireless signal.
iii. Designated System Administrator should regularly search for rogue or unauthorized wireless access points;
iv. Once a device is reported missing, Designated System Administrator should modify the encryption keys and SSID.

5.2.2 Network Design and Technical Controls

The Designated System Administrator should ensure the following:

i. Change product default access point configuration settings.
ii. Disable all insecure and unused management protocols on access points.
iii. Enable and configure security settings to make sure that unauthorized users do not gain access to MoF wireless network.

iv. Ensure all wireless connections are connected to the security equipment (e.g. firewall, router).
v. Activate logging features and redirect all log entries to a logging server. The log records should be checked regularly.
vi. Install NIDS or NIPS to monitor the wireless networks;
vii. Deploy secure wireless technologies on top of wireless network.
viii. Segment the access point's coverage areas to balance the loading to minimize the probability of Denial-of-Service (DoS) attack.

5.2.3 Client Controls

The Designated System Administrator should:

i. Activate personal firewall on wireless clients (e.g. laptops, PDAs) that are used outside Network boundary.
ii. Turn off sharing at wireless clients.
iii. Keep strict control of the wireless interface cards (e.g. PCMCIA card for laptop) as access credentials such as SSID and/or encryption key are commonly stored on the card.
iv. Enable wireless connections only when users need them and disable them when they are no longer in use.
v. Follow the guideline protection against computer virus and malicious code.

The head of the ICT unit will be responsible to ensure the guidelines for wireless network security are adhered to.

5.3 Internet Security

MoF should strike a balance between taking advantage of the Internet and maintaining security and confidentiality based on the following requirements:

i. Browsing of Internet sites containing pornographic, obscene, and immoral or any other inappropriate content is prohibited.
ii. ICT unit should ensure that MoF network is protected from harm and danger that come with the use of the internet.

iii. MoF internet service/connection should not be used to perform illegal acts and unauthorized activities.
iv. The ICT unit should strive to maintain a fast, efficient and secure internet connection. To maintain such quality, services such as media streaming and downloading, social network sites and online games are discouraged during working hours.
v. All access to the internet should be routed through web filtering hardware and monitoring software.
vi. All temporary staff and visitors are bound to this guideline.

The head of the ICT unit will be responsible to ensure the adherence of the guidelines for internet security.

5.4 E-mail Security

E-mail communication is very efficient and cost effective at communicating in written and multimedia form. E-mails can reach global masses in an instant. It is this ease of use that makes email communication open to abuse. In addition, email communication has the potential to advance illegal and unlawful course, as well as transmit harmful content such as computer viruses. It is for this reason that measures must be put in place to ensure that email communication is used responsibly based on the following requirements:

i. Users should use e-mail responsibly and preferably for official matters.
ii. Users should not open or forward any e-mail from unknown or suspicious sources.
iii. Users should not copy or forward chain e-mails. Chain emails can disrupt email services and other internet services on MoF network.
iv. If users suspect or discover e-mail containing computer viruses or phishing attacks, they should report the incident to the designated Information Security Officer.
v. The e-mail system should not be used to commit unlawful and illicit acts.

vi. The users should avoid publishing e-mail address to unknown individuals or exposure of users' credentials by filling forms from dubious links and websites.

vii. Users should use separate e-mail addresses different from their office e-mail addresses when participating in public newsgroup or chat rooms, to avoid their office e-mail addresses and/or mail systems to become a target of spam.

viii. Users should not reply to spam because most return addresses are not legitimate and would only result in the generation of non-delivery messages thus increasing the amount of undesired traffic.

ix. Users should control spam by using e-mail filtering tools in e-mail software that allow users to block or screen out spam by defining some simple filtering rules.

x. User should not send e-mails using another person's e-mail account.

xi. Only encryption authorized by the MoF should be used to encrypt e-mails.

xii. Mail systems should have a mechanism to scan e-mail attachment for viruses and other malicious before sending or downloading.

The head of the ICT unit will be responsible to ensure the adherence of the guidelines for email security.

5.5 Protection against Cyber Attacks

In addition to network, internet and e-mail protections the following guidelines should be adhered to in order to protect against cyber attacks:

i. Pattern analysis should be used to identify changes in on-line activity that may indicate a cyber attack.

ii. ISP and designated systems administrator should ensure that the following categories of data are retained:

- Data necessary to trace and identify the source of a communication.
- Data necessary to identify the destination of a communication.

- Data necessary to identify the date, time and duration of a communication.
- Data necessary to identify the type of communication.
- Data necessary to identify users' communication equipment.
- Data necessary to identify the location of mobile communication equipment.

The head of the ICT unit will be responsible to ensure the adherence of the guidelines for protection against cyber attacks.

5.6 Protection against Computer Viruses and Malicious Code

Potential damages may include modifying data, destroying data, stealing data, allowing unauthorized access to the system and popping up unwanted screens. Protection against Computer viruses and malicious code should be done based on the following requirements:

i. Designated MoF System Administrator should enable real-time detection to scan computer virus and malicious code for active processes, executables and document files that are being processed.
ii. Designated MoF System Administrator should scan any files on electronic or optical media, and files received over networks against computer virus and malicious codes before use.
iii. Designated MoF System Administrator should make sure e-mail server is configured such that attachments and downloads are automatically scanned against computer virus and malicious code before use.
iv. Before installing any software, Designated MoF System Administrator should verify its integrity (e.g. comparing checksum value) and ensure it is free from computer virus and malicious code.
v. Installation of any software or file received via e-mail or downloaded from web browsing should be approved by MoF relevant authority.
vi. Users should always boot from the primary hard disk. Booting workstations from removable storage device should not be done without permission.

vii. Designated MoF System Administrator should conduct daily update of the virus definition files to minimize the risk of infection from new viruses.

viii. Designated Information Security Officer should prepare and implement user's awareness training programs on virus issues.

5.7 Responding to Virus Incidents

i. The Designated Information Security Officer should take all relevant details from the caller about the nature of the virus, its possible origins, and any previous alerts.

ii. The Designated Information Security Officer(s) should scan the relevant file(s) with antivirus software, to determine whether the virus has been immunized.

iii. The Designated Information Security Officer should establish whether the virus may have infected others and, if so, respond accordingly; if necessary by closing down workstations and even parts of the network.

iv. Users should communicate details to the designated Information Security Officer, seeking any additional guidance as necessary.

v. The Designated Information Security Officer should communicate new virus alert to warn personnel about the incident and the appropriate response.

vi. The Virus Incident Response Procedures will be documented if a virus (or other malicious code) affects MoF critical systems.

vii. Ability to respond to virus incidents should be regularly reviewed and tested. Failure to respond appropriately to a virus incident can rapidly result in multiple systems failures and continued infection.

5.8 Protecting Against Internal Attacks (Insider Threats)

In order to reduce the incidence and possibility of internal attacks, access control and data classification policies and procedures are to be maintained at all times and periodically reviewed based on the following requirements:

i. Enforce separation of duties and least privilege on the system.
ii. Log, monitor and audit employee actions on the system.
iii. Conduct periodic security awareness training to all employees.

The head of ICT unit will be responsible for network, internet and email security controls mentioned above.

6. SOFTWARE SECURITY MANAGEMENT

Information systems used at MoF shall either be developed internally or acquired as per MoF requirements. Organizational security may be compromised if software development or acquisition will not consider security issues.

All software development, acquisitions, deployment and usage at MoF should be coordinated centrally by ICT Unit to ensure conformity to predefined standards.

The following are measures that are to be considered in software security management at the Ministry of Finance.

Software Development

i. Security features should be considered on all MoF software development. These features include:
   - Segregation of duties.
   - Proper authentication and authorization.
   - Proper session management.
   - Input validation.
   - Data authenticity and integrity.

ii. Software should be tested so that the logical errors are rectified accordingly.

6.1 Software Acquisition

i. On acquiring software, proper procurement procedures should be followed as stated in the Public Procurement Act and its Regulations.
ii. All software acquired by MoF should have documentation manuals and bear legitimate licenses.

iii. Usage of primary and secondary license should not be interchangeable.
iv. Delivery and guaranteed of functionality of acquired software should be the responsibility of the supplier.
v. MoF ICT Unit should ensure proper management of licenses for the software acquired.
vi. Acquired critical software should be covered by escrow agreement to ensure continuity.
vii. Use of open source software should adhere to the Government Circular number 5 of 2009 of Permanent Secretary PO-PSM.

The head of the ICT unit will be responsible to ensure the guidelines for software acquisition are adhered to.

6.2 Software Deployment

Software deployment involves the installation and testing of software.

i. Testing of the software to be deployed should be conducted sufficiently such that security is not compromised.
ii. The ICT staff should prepare a well documented test plan before software installation. The plan should be approved by the supervisor.
iii. Installation and activation of software should follow manufacturer's security standard, provided that they comply with MoF security standards.
iv. All software to be deployed at MoF should be free from virus or malicious code.
v. Installation should be done properly.
vi. Any deployment of software in MoF environment should be approved by relevant authority.

The head of the ICT unit will be responsible to ensure the guidelines for software deployment are adhered to.

6.3 Software Customization

i. All software customizations should comply with user department requirements and MoF security guidelines.
ii. Designated officer should verify that need for a particular customization has been met.

6.4 Software Usage

i. Software should be used for intended purpose as stipulated in terms and conditions of the software.
ii. Before an employee is permitted to use a particular software, the designated department should instruct users on the proper usage of the particular program.
iii. Designated department should inform users on terms and conditions included in the license agreement accompanied by the program.

6.5 Systems Integration and Interoperability

i. In order to ensure confidentiality, integrity and availability of data and information, all MoF information systems should be integrated.
ii. Any new system should be compatible and interoperable with existing system without compromising organizational security.
iii. Different existing systems should be integrated by adhering to ICT security standards.

The head of the ICT unit will be responsible to ensure the guidelines for systems integration and interoperability are adhered to.

6.6 Software Change Management

Software Change Management is the process of planning, organizing, controlling, executing and monitoring changes that affect the delivery of ICT services. It encompasses all components and activities required to direct

additions, modifications and deletions. Software change request should be submitted for approval using Change Request Form (Appendix C).

6.6.1 Implementing New or Upgraded Software

The implementation of new or upgraded software must be carefully planned and managed as a project for critical systems. Security risks will be minimized basing on the following requirements:

i. All staff involved in installing the new software or upgrade should be suitably qualified, trained or supervised.
ii. A suitable contingency plan should be in place in case of failure of the new software.
iii. Systems Administrator should properly test new or upgraded software before using in a live environment based on approved pre-designed test plan.
iv. Upgraded software versions should offer at least the current level of security safeguards.
v. System owner should decide the specific criteria and cut-off date, which will trigger a reversion.
vi. Regression Testing should test all the key features of the software not just those which have been changed or updated.
vii. System owner should always ensure that an upgraded software version can read and write files in the older format.
viii. Major upgrades of operating system version on the MoF servers should be avoided unless there is a genuine reason for the upgrade.

6.6.2 Applying Patches/Service Packs

If a patch is applied incorrectly or without adequate testing, the system and its associated information can be placed at risk, possibly corrupting live data files. Patches applied to resolve software bugs shall only be applied when verified as necessary and with authorization from the user department based

on the following requirements:

i. Patches should be from a reliable source and are to be thoroughly tested by the system administrator before use.
ii. System administrator should verify that the patches are necessary and come from an authorized source, normally the software manufacturer or vendors.
iii. System administrator should ensure that updates to the system documentation are received with the patches.

6.6.3 Responding to Vendor Recommended Upgrades to Software

The decision whether to upgrade MoF's software is to be taken only after consideration on the associated risks and costs of the upgrade against the anticipated benefits and necessity for upgrade. Vendors' proposals for upgrade of operating systems or application programs should be appraised taking the following into account:

i. The upgrade is in line with overall strategy for MoF system development.
ii. The vendor's motives for recommending the upgrade are ascertained.
iii. Contract should stipulate vendors' role on supporting (old) version.

6.6.4 Capacity Planning and Testing

Capacity Planning is the determination of the overall size, performance and resilience of a system. New and upgraded software must be planned and tested for expected future capacity and subjected to stress testing based on the following requirements:

i. It should demonstrate a level of performance and resilience which meets or exceeds the technical and business requirements of MoF systems.

ii. New and upgraded software should be subjected to transaction volumes that simulate or exceed expected future live requirements.
iii. Any areas where system testing has not been representative of the live environment should be identified, and the resultant risks evaluated.

6.6.5 Parallel Running

Parallel Running is the process of running a new or amended system simultaneously with the old system to confirm that it is functioning properly before use. This process should base on the following requirements:

i. Normal system testing procedures should incorporate a period of parallel running prior to the new or upgraded software being acceptable for use in the live environment.
ii. A parallel run phase should be incorporated in the User Acceptance Test Plan.
iii. In a scenario where two systems are running parallel, the maximum time for parallel running should not exceed six months.
iv. Where results differ between the old and new system, the old system should continue to be used until the new system is up and running, or otherwise agreed as acceptable.

6.6.6 Emergency Request Change

On occasion, changes of an “emergency” or critical nature may be required to quickly address production issues arising in case of emergency. Changes should be rectified urgently while still maintaining the proper levels of approval, logging, monitoring, communication and closure of all change related activities.

7. BUSINESS CONTINUITY MANAGEMENT

The Business Continuity Plan identifies the organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization. Components of Business Continuity are risk management, incident management and disaster recovery planning as described below.

7.1 Risk Management

This section will address major components of Risk Management which are Risk Identification, Risk Assessment, Risk Evaluation and Risk Treatment.

7.1.1 Risk Identification

Information security officer in collaboration with user department should identify ICT security risks facing organizational assets.

7.1.2 Risk Assessment

During Risk Assessment exercise, the following tasks will be carried out:

i. Information security officer should be aware of Organization objectives.
ii. Information security officer should prepare Information Systems Assets Inventory. This inventory is a result of the risks identified by risk experts from user departments.
iii. Information security officer should perform regular ICT security risk assessments and audits to identify security vulnerabilities.

7.1.3 Risk Evaluation

Information system security officer should evaluate risks based on

magnitude and impact of risks for example, low, moderate, high, and extreme.

7.1.4 Risk Treatment

Information system security officer should develop a feasible and cost effective risk treatment strategy.

7.1.5 Risk Monitoring and Review

Whatever the risk treatment option selected, information security officer should keep on monitoring and review risk management plan continuously.

7.2 Incident Management

Any event which suggests that the confidentiality, integrity and availability of the information has been compromised can be considered a security incident. When a security incident occurs, it is important to respond calmly and follow a logical procedure.

i. Should any employee suspect an incident the details of the act should be immediately reported to the information security officer. Action will then be taken to try to prevent a security breach happening or continuing.
ii. Information Security officer should have appropriate tools to track, identify and document security breach incidents.

7.3 Disaster Recovery Planning

MoF Disaster Recovery Site (DRS) shall be a real-time based backup site in a remote physical location containing ICT equipment configured and ready to run MoF Systems. DRS team should be trained and assigned the task of maintaining and executing the Disaster Recovery Plan. MoF Disaster Recovery Plan should constitute of the following definitive steps:

i. Back-up and disaster recovery plan should be put in place for organizational valuable data.
ii. Information system security officer should recommend a data backup and business continuity solution.
iii. Information system security officer should align and communicate the Ministry data back-up and disaster recovery planning policies to user departments.
iv. Copies of the MoF databases should be in near real time backed up onto the DRS servers**.**
v. Database administrator should backup all critical systems to the offsite as per disaster recovery plan.
vi. The system owner should authorize execution of disaster recovery plan after disaster declaration.

7.4 Back-up and Restoration Procedures

In order to ensure business continuity, back up of all critical systems should be maintained. The retention period for essential information, and also any requirement for archive copies to be permanently retained, should be determined. The Information system security officer in collaboration with system administrator should adhere to the following requirements:

i. Ensure that all essential information and software can be recovered following a disaster or media failure.
ii. Data backup plan and procedures for each application/system are developed and enforced.
iii. A minimum level of backup information, together with accurate and complete records of the backup copies and documented restoration procedures, are stored in a remote location, at a sufficient distance to avoid being affected by the same disaster that may hit the main site.
iv. Backup media are regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.

v. Restoration procedures are regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

vi. User Data, Database and System state are backed-up regularly, normally once per day at the end of the working day.

vii. The contents of the back-up tape/disk are verified and ensured that the data has been saved. If the backup fails the process need to be reconfigured and repeated.

viii. Back-up files are placed immediately into secure storage on-site and on the remote site.

ix. Execution of the backup procedures needs to be rotated between responsible staff.

x. Back-up procedures are documented in the Information Security Procedures Manual.

xi. All back-up files are clearly labeled and held in secure locations.

xii. Data restoration should be supervised by the ICT Unit.

8. MANAGEMENT OF THIRD PARTIES

All external organizations or individuals who wish to supply services to Ministry of Finance will be bound to follow these ICT security guidelines as part of their contractual terms. Management of third parties include issues on third party verification, service level agreements, outsourcing, cloud computing services, equipment leasing, maintenance and support services, and lastly issues pertaining to Internet Service Providers (ISP's).

In a scenario where vendors fail to deliver service as per Service Level Agreement, disciplinary measures will be taken upon them according to terms and conditions as stipulated in the contract.

8.1 Third Party Verification

i. All third parties should be verified as being legitimate before being allowed access to any of the Ministry's ICT resources.
ii. A register should be kept showing when, why and by whom access was requested and if it was granted or not.
iii. A third party should complete Confidentiality Agreement Form (Refer Appendix B)
iv. In case a Third party need to access MoF systems they should be assigned new logon details (username and passwords) and relevant access privileges.
v. Any created user log on details to allow access to MoF systems should be changed as soon as access is no longer required.

The head of the ICT unit will be responsible with the above guidelines.

8.2 Outsourcing

Prior to entering into an ICT outsourcing arrangement, care should be taken to ensure that process will not compromise organization objectives, policies and standards. Thus, outsourcing process should base on the following

requirements:

i. Outsourcing activities should consider risks and security concerns.
ii. MoF should develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the technology service provider. This should include termination plan and identification of additional or alternate technology service providers for such support and services.
iii. Outsourced services should be regularly reviewed and analyzed for inappropriate or unusual usage, during the life of the contract.
iv. Any problems discovered during the implementation of the outsourced information system services, solutions should be documented and used to improve the controls.
v. Protection of personal information and organizational data by ensuring appropriate and effective confidentiality agreements are in place.
vi. Compliance with information, security and privacy policies, laws and regulations.
vii. Access Protocols and remote access controls should be met by the provider, its staff and contractors.

The head of the ICT unit will be responsible with the above guidelines.

8.3 Cloud Computing Services

Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. While the cloud may be flexible and cost-efficient, lack of data safeguards and compliance standards makes security the largest hurdle to leap. Based on this, cloud computing service are not advisable unless need arises due to unease surrounding the external management of security based services and be guided by the following requirements:

i. The SLA's should be practical and state specific remedies that apply

when they are not met.

ii. The sensitivity of data, data segregation, privacy, bug exploitation and recovery should be examined.

iii. Cryptography mechanisms should be used to ensure the authentication, integrity and confidentiality of involved data and communications.

iv. Examine if cloud computing vendor is "Trusted Cloud Computing Vendor". A Trusted Cloud Computing Vendor is the one who:

- Has high level confidentiality
- Uses server and client authentication
- Uses security domains
- Uses cryptographic in data separation
- Uses certificate-based authorization

8.4 Equipment Leasing

MoF may wish to enter into operating leases agreements of ICT equipment with service providers. Under these agreements, the leasing company can decide what to do with its equipment as it does not belong to MoF following contract expiration. In this situation, the following issues need to be observed:

i. All data in leased equipment should be removed "Permanently" before the equipment is taken to the leasing company.

ii. All configurations, set to the leased equipment should be erased and returned to default industrial state before the equipment is taken to the leasing company.

iii. Service level agreements with leasing companies should take into account part (i) and (ii) above.

8.5 Maintenance and Support Services

i. Maintenance should be done on regular basis. The contractor should

take all measures to protect from data loss during maintenance operations.

ii. In addition to guideline 8.1 (Third Party Verification), all maintenance of ICT equipment and software should be done at MoF and under the supervision of ICT unit personnel.

iii. In case, the damaged Computer Systems need to be taken to the contractor, the following should be examined;

- The storage media within the systems should be removed before the equipment is taken to the contractor.
- If the storage media is needed, then the sensitivity of data within the media should be examined and for high sensitive the ICT staff should accompany the contractor.

iv. If actual operational data is needed by contractor during maintenance or support operation then data should slightly be changed. For complex databases specific change queries should be required.

v. The maintenance of ICT equipment and software should be allowed where necessary and the login should be governed by guidelines under "Remote access".

vi. MoF ICT department/unit should ensure that the equipment does not contain sensitive live data when hardware is taken by the service provider for servicing/ repairing.

vii. Service contracts with all service providers including third-party vendors should include confidentiality clause and right to have information system audit conducted (internal or external).

8.6 Internet Service Provider

i. The ISP should agree not to disclose the contents of MoF electronic communications to any other third party.

ii. The ISP should have redundant links.

iii. All protocols and methods used should be RFC compliant and conform to TCRA standards.

8.7 Third Party Contract Management

Designated contract management expert should manage all ICT contracts. The following tasks should be carried out:

i. Organizational records and documents should be examined to ensure third-party providers use security controls in accordance with laws, regulations, standards, directives, and agreements.
ii. Suspected violations or suspicious activities by third parties are investigated and the findings are reported to appropriate authority.
iii. Any problems discovered during the implementation of the outsourced information system services, solution should be documented and used to improve the controls.
iv. Report on the percentage of third-party relationships that have been reviewed for compliance with information security requirements.

9. TRAINING, AWARENESS AND SUPPORT

Adequate training of all personnel is critical to the effective implementation of information security. Security awareness and training activities should be ongoing to further demonstrate management's commitment to information security. The Management should be proactive in communicating its expectations and requirements to its personnel, as well as in prescribing disciplinary action for non-compliance. Users should be appropriately trained to perform their tasks prior to access to systems and information being granted.

To give appropriate security training to MoF users, the users have been categorized into technical users, end-users and temporary employees/trainees.

9.1.1 Technical User

i. Technical users should be trained on security aspects for a new procured software and hardware.

ii. Regular training should be conducted to technical users; this includes systems analysts, designated system administrators and information security officers on the use of patches for existing software.

iii. Designated Information System Security officer should monitor and review the level of information security knowledge of technical and operation staff on regular basis. This can be achieved by introducing a bi-annual self-assessment form.

9.1.2 End User

i. End users should be trained on security aspects for a new procured software and hardware.

ii. End users should be given appropriate information security trainings on the latest security threats and information security techniques on regular basis.

9.1.3 Temporary Employees and Trainees

Temporary employees and trainees such as field students should adhere to the following requirements:

i. Attend induction training on security matters and sign non-disclosure agreement prior to accessing Ministry of Finance information systems.
ii. Attached to a selected location.
iii. Given limited access to the system.

9.2 Security Awareness Program

i. Awareness program that focus on ICT security related issues should be developed by the ICT unit.

ii. Users of ICT resources should be trained and provided with copies of ICT Security Guidelines and procedures to make them aware of potential security concerned and to understand their responsibility to report security incidents and vulnerabilities.
iii. Updates to procedures should be regularly publicized to users for example the use of posters, leaflets, fliers and brochures. Moreover, training seminars for new threats should be considered seriously.
iv. User should be made aware of the importance of the information processes, the associated threats, vulnerabilities and risks and understand why controls are needed.

9.3 User Support

i. The ICT Unit should ensure proper use of ICT equipment and programs.
ii. All Users should immediately report to the ICT Unit through the help desk office on occurrence of any security threat.

10. HARDWARE RETENTION AND DISPOSAL

Hardware Retention and Disposal define procedures for persistent data or information management in order to meet legal and business data archival requirements. The process should be governed by the Government Circular Number 6 of 2009 of PS PO-PSM. The following requirements for disposing of MoF ICT hardware should be followed:

i. Information should be moved to another system, archived, discarded or destroyed in accordance with MoF's data retention procedures.
ii. When ICT hardware is disposed of, the system administrator should ensure that all data/information in that hardware has been erased or destroyed.
iii. Disposal of MoF's hardware should be approved according to the Public Procurement Act and its Regulations.
iv. When disposing a device, the system administrator should make sure that the device that has been disposed of has no usable residual data and even advanced tools should not be able to recover erased data. Therefore, hard disks should be removed and destroyed.

11. PERSONNEL SECURITY

Personnel security covers guidelines that deal with MoF employees as per Public Service Acts, Regulations, Circulars and Directives. This chapter elaborates on guidelines that pertain to segregation of duties as well as personnel management.

11.1 Segregation of Duties

i. Clear roles and responsibilities for the security of information and information systems, should be developed and documented. This is to ensure that every ICT staff is allocated in known field of work according to the set scheme of service.
ii. The documented responsibilities (job description) should be assigned to specific individuals.
iii. All personnel should be made aware of their responsibilities and obligations by signing their job descriptions. This will help to reduce risks resulting from errors or intentional or unintentional breach of security due to the inconsistency of information.

11.2 Personnel Management

This area deals with introducing new users to the system, maintaining the users through the whole period of working time to termination or removal from the system. These processes require the following:

11.2.1 Employee Engagement

The head of the user department should provide information for a new employee to ICT Unit for them to be registered into the system.

11.2.2 Employee Workplace Practices

i. Human resource (HR) officer should provide updated information of existing employees to the ICT Unit on regular basis.
ii. System administrator should act upon the updated information of employees from HR officer. The system administrator should enquire updated employees' information from HR officer if the information is not received on time.
iii. All employees who are on leave, their system account should be deactivated and reactivated when they report back to office.

11.2.3 User Account Termination

Employee account termination may arise due to employment suspension, termination, leave, retirement, death, transfer and job change.

The following are measures to be taken by HR and ICT department during termination process:

i. Human resource officer should provide information to the ICT department concerning employees who are leaving the organization on regular basis.
ii. The system administrator should ensure that the system account for employee who is leaving the organization is terminated.
iii. All ICT assets for any terminated staff should be returned to respective department or unit.

12. MONITORING AND EVALUATION

Monitoring and Evaluation is a tool that ensures application of ICT within MoF complies with this Guide. In a scenario whereby the ICT activities within MoF appears to be not in line with this Guide the tool will help to get ICT operations back on the right track. Monitoring and evaluation process will also address new information security challenges that may arise due to technological advancement. This would eventually initiate a review process of this ICT Security guideline so as to take on board new security changes.

For successfully monitoring and evaluation exercise, MoF ICT Unit should perform the following:

i. Oversee all information on security issues at the Ministry of Finance.
ii. Monitor regularly these Guidelines to ensure that all users are adhering to them.
iii. Distribute and interpret the ICT Security Guidelines to MoF employees and third party entities.

ICT Unit should provide feedback to ICT Steering Committee on the issues, obstacles, challenges and achievements made during implementation of the Guide. In addition, monthly, quarterly, semi annual and annual reports will be prepared for the ICT Steering Committee to brief them on various issues relating with ICT security.

REFERENCES

i. National ICT Policy 2003
ii. National Security Act No. of 1970
iii. Tanzania Police Force, ICT Security Procedures
iv. Records & Archives Management Act. No. 3 of 2002
v. GoT Circular No. 5 of 2009 of Permanent Secretary PO-PSM
vi. GoT Circular No. 6 of 2009 of Permanent Secretary PO-PSM
vii. GoT Circular No. 1 of 2011 of Chief Secretary
viii. Public Service Act No. of 2003

Appendix A-

Ministry of Finance
Accountant General Department
Systems Development Unit

IFMS USER LOGIN ID/SERVICE REQUEST FORM

Reference Number:

SECTION A: (*To be Filled in by prospective User)*

Ministry/Dept/Sub-Treasury/RAS: **Vote:**

Department: **Section:**

Please cross the respective System/Software for the Login to be Created/ Activated / Deleted

☐ Network Access	☐ Active Planner	☐ Crystal Reports
☐ Epicor	☐ CSDRMS	☐ eintelligence Suite
☐ IFMS PE	☐ FRX Financials	☐ Import manager

Please provide us with the relevant information:

Request For a **NEW** Login ID

	First Name	Middle Name	Surname
Full Name			
Title/Description			
Existing IFMS ID (if any)			

Request for ☐ **RE- ACTIVATE,** ☐ **ENABLE** or ☐ **DISABLE** existing Login

Login Name	Re-Activate	
	☐ With New Password	☐ With No Password

Requested by: _____

Signature :_____

Approved by: _____

Title: _____

Signature: _____

Date and Stamp: _____

Page 1 of 4

IFMS USER LOGIN ID/SERVICE REQUEST FORM

FOR INTERNAL USE ONLY
SECTION B: (*To be filled in by the system administrator*)

First name: _____ Last name: : _____

Login ID: _____

Logon Hours:

☐ Regular (8:00 a.m to 6:00 p.m)

☐ Special. Please specify:

_____

User Role:

☐ Data Entry User
☐ Approval User
☐ Report User
☐ Network User

Database access-Access level *(As determined by User Matrix)*

Company name/Vote code	Access level

Approved by: _____

Title: _____

Signature: _____

Date: _____

Created by: _____

Signature: _____

Date: _____

SECTION C: ***(To be filled in by SDU technical staff)***

User Login name:_____
(Should be in Format of First letter of First Name followed by the Surname)

Indicate the actions taken by ticking the appropriate box:

☐	User must change password at next logon	☐	Account disabled
☐	User cannot change password *(should not be ticked)*	☐	Account Locked
☐	User cannot change password *(should not be ticked)*		

Member of: ***(Record group membership here)***

1.	2.

Created by:_____

Signature:_____

Date:_____

SECTION D: ***(To be filled in by User Whose Account has created or reactivated)***

Password received and Changed By: _____

Date and Signature: _____

Comments: (Record any other necessary information here i.e. special rights/privileges granted)

SECTION E: To be filled in by the documentation officers

Received By: _____

Date: _____

Reference number : _____

IFMS USER LOGIN ID/SERVICE REQUEST FORM

USERS' INSTRUCTIONS ON HOW TO FILL IN THE FORM

One form should always be filled per user, in duplicates. The form must be approved, signed and where possible stamped by the a recognized authority of the user department.

The Form has five sections: **A**, **B**, **C, D and E**
Section A and D should be filled in by users requesting a login ID and related services.
Sections **B**, **C** and **E** are for internal use of the Accountant General's Department.

Section A: Should be filled prospective user and the authority of the department from where the user belongs

Section D: To be filled in by Users to acknowledge receipt and changing of the network password.

Below is a short description of some fields of the Form:

1	Reference number	This is the number to be allocated by the SDU in the format of date/request number
2	Network Access	Access related to the AGD Domain or network
3	Epicor	Access related to the main IFMS application Epicor
4	IFMS PE	Access related to IFMS plan Extension module
5	Active Planner	Access related to Active planner application
6	CSDRMS	Access related to the CSDRM system
7	FRX Financials	Access related to FRX module
8	Crystal reports	Access related to Customized Crystal reports
9	Import manager	Access related to import Manager Module
10	eintelligence Suite	Access related to data warehouse client
11	Title/Description	Should cover the user's job title and role in the system e.g. Assistant Accountant/Data Entry
12	Existing IFMS ID	The network ID for an existing user or a user who has worked with the AGD domain before
13	RE-ACTIVATE	Selecting this option leads to your login IDs being activated for those Login IDs that may be locked or those login IDS that might have expired or login IDS whose password have been forgotten
14	ENABLE	Selecting this option leads to a disabled login IDs being enabled and reactivated
15	DISABLE	Selecting this option will lead to the Login ID being disabled
16	Requested by	This must be the name of the user who request the services
17	Approved by	This must be the name of the Accounting officer if the User request is for a new Chief Accountant or regional Accountant. For all other users this must be the head of department where the user resides

Appendix B-

Confidentiality and ICT security Compliance – Non employee

PF No……

MoF regards security and confidentiality of data and information to be of utmost importance. Each consultant, practical training student, or any other person granted access to data and information holds a position of trust and should preserve the security and confidentiality of the information he/she uses. This form is used to acknowledge and agree receipt of, and compliance with the MoF ICT Security Guideline.

I----------, of ----------
do hereby solemnly state as follows:-

1. That I have carefully read and understood the contents of the "ICT Security Guideline", copies of which were supplied to me by the ICT Unit/MoF Management.

2. That I understand and agree that any computers, software, and storage media provided to me by the MoF contains proprietary and confidential information about MoF and its customers or its vendors, and that this is and remains the property of the MoF at all times.

3. That I will not access or attempt to gain access to any computer, computer account, network or files without proper and explicit authorization, and further that I will inform the MoF management immediately, should I become aware that such access has taken place.

4. That I agree that I should not copy, duplicate otherwise disclose, or allow anyone else to copy or duplicate any of this information or software except in the circumstances where I am authorized so to do by the MoF management.

5. That I understand that I am to restrict my retrieval and other computing activities only to a date on which I have been specifically permitted to access as related to my assigned duties and using only functions and utilities which I have been authorized and trained to use.

6. That I understand that my account and password are issued for my exclusive use only, and I am responsible for the security thereof. I will not authorize or facilitate the use of my account or files by any other person, nor will I divulge my password to any other person.

7. That I agree that if I don't adhere to these MoF Security Guidelines, stern legal measures shall be taken against me.

Name:……

Date:……

Signature:……

FOR OFFICIAL USE ONLY:

Endorsed **By:**

Name:……

Position:……

Signature:……

Date:……

Change Request Form

Change Request Form (Sample)

Change Description/ CR Filename:					
Change Request No.:		**Project:**			
Requested by:				Date:	
Department/ location				Telephone:	
Description of the change:					
Change needed by (date):					
Reason for the change:					
Requestor Sign off:					
Approval of Request:					
Change Impact Evaluation (use page 2 for details)					
Change Type		Application		Database	
		Hardware		Procedures	
		Network		Security	
		Operating System/Utilities		Schedule Outage	
Change Priority		Urgent	**Change Impact**		Minor
		High			Medium
		Medium			Major
		Low			
Environment(s) Impacted:					
Estimated Resources: [cost or effort]					

CTS Internal:		External:	
Resource requirements: (personnel , h/w, s/w)			
Test Plan Description			
Rollback Description			
Change Approval or Rejection			
Change Request Status		**Accepted**	**Rejected**
Comments:			
Change scheduled for (date):			
Implementation assigned to (names):			
Management Sign off:			
Change Implementation			
Staging test results:			
Implementation test results:			
Date of Implementation			
Implementer Sign Off		Date	