REPUBLIC OF NAMIBIA

MINISTRY OF FINANCE

INFORMATION TECHNOLOGY DIVISION

ICT SECURITY POLICY

FOREWORD

Security is defined as "the state of being free from unacceptable risk; or the degree of protection against danger, loss, and criminals". In terms of Information Technology, security can be defined as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction".

Information Communication Technology (ICT) has taken the world by storm resulting not only in benefits for the individual and corporations but also an increase in the breach of security. The widespread implementation and use of computers and networks and distributed client/server processing environment(s) are accompanied by new risks and exposures.

The utilization of ICT across the world has resulted in making it a strategic tool to achieve social economic development goals globally which is greatly facilitated by the globally connected networks, i.e. the Internet. The increasing capacity of ICT has further been empowered by the growth of a global network of computer networks i.e. the Internet.

ITC 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.

The Ministry of Finance (MOF) has taken advantage the advancement and benefits of ICT to develop and implement several ICT systems for effective and efficient service delivery; both for itself and also for its sister ministries.

The Ministry acknowledges the security risks, threats and attacks associated with the utilisation of ICT systems both within MOF and through its connectivity to other agencies; as well as its obligation to ensure the implementation of appropriate security mechanisms to protect all ICT resources that will warrant the integrity, availability and confidentiality of data.

Furthermore, the Ministry established the Ministerial ICT Steering Committee in the year 2006 to oversee proper utilization of ICT resources in the Ministry as well as to monitor all ICT activities while ensuring that these activities are in line with set procedures and follow best

practice as the unauthorised access to or modification of, important and/or sensitive MOF data can far outweigh the cost of the equipment itself.

This policy 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.

The policy applies to all Ministry of Finance employees, consultants and any other party who uses MOF ICT resources in any form. It should be noted that where an employee or non-employee fails to comply with these policy statements; Disciplinary measures will be taken against him/her as per Public Service Acts, Regulations, Circulars and other Government Directives.

It is therefore required that upon the date of taking up employment with the Ministry, in any form, familiarization with the content of this policy and signing of the confirmation form is done.

PERMANENT SECRETARY – MINISTRY OF FINANCE

TABLE OF CONTENTS

REVISION HISTORY

ICT Policy (Entire Document):	January 2005
ICT Policy (Entire Document):	April 2005
ICT Policy (Entire Document):	September 2010.

ACRONYMS AND ABBREVIATIONS

BCP	Business Continuity Plan
CCTV	Closed Circuit Television System
CD	Compact Disk
CD-ROM	Compact Disk, Read-Only Memory. A type of storage device that looks just like an audio CD however, you can't save or change files on a CD-ROM, only read them
CPU	Central Processing Unit; the brains of the computer. The CPU interprets and executes the actual computing tasks
CRAN	Communications Regulatory Authority of Namibia
DAdmin	Director of Administration
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
GRN	Government of the Republic of Namibia
HR	Human Resource
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPX	Internet Protocol Exchange
ISP	Internet Service Provider
ITD	Information Technology Division
LAN	Local Area Network
LGAs	Local Government Authorities
MAC	Media Access Control
OMAs	Offices, Ministries and Agencies
MOF	Ministry of Finance
NIDS	Network Intrusion Detection Systems
NIPS	Network Intrusion Protection Systems
OPM	Office of Prime Minister
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
RFC	Request for Comments
SBAS	Strategic Budget Allocation System
SLA	Service level Agreement
SSID	Service Set Identifier
TLS/SSL	Transport Layer Security/Secure Socket Layer
UPS	Uninterruptible Power Supply

User ID	User Identification
VPN	Virtual Private Network
WAN	Wide Area Network

DEFINITION OF TERMS

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

Address Resolution: Conversion of an IP Address to the corresponding low-level physical address.

Application: a combination of hardware and Software that provides shared access of programs or information to multiple Workstations and/or Users, including, but not limited to, Business Systems, Messaging Systems, Database Management Systems and Document Management Systems. Software that lets users do relatively complex tasks, as well as create and modify documents. Common application types include word processors, spreadsheets, database managers, and presentation graphics programs.

Backbone: Network used to interconnect several networks together.

Bandwidth: The capacity of the transmission medium stated in bits per second or as a frequency. The bandwidth of optical fiber is in the gigabit or billion bits per second range, while Ethernet coaxial cable is in the megabit or million bits per second range.

Booting: Starting up a computer via the power switch, which loads the system software into memory. Restarting the computer via a keystroke combination is called rebooting or a warm boot.

Broadcast: A packet whose special address results in its being heard by all hosts on a computer network.

Browser: A program that enables you to access information on the Internet through the World Wide Web.

Cloud computing: 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.

Confidential Information: information of whatever nature, which has been, or may be obtained by the Ministry of Finance, whether in writing or electronic form or pursuant to

discussions between the Ministry of Finance and IT Resource vendors, or which can be obtained by examination, testing, visual inspection or analysis, including without limitation, scientific, business or financial data, know-how, formulae, processes, designs, customer lists, price lists, studies, findings, computer software, hark inventions or ideas, analysis, concepts, compilations, studies and other material prepared by or in possession or control of which contain or otherwise reflect or are generated from any such information as is specified in this definition.

Configuration: 1. The Departments that make up a computer system (which model and what peripherals). 2. The physical arrangement of those Departments (what's placed and where). 3. The software settings that enable two computer Departments to talk to each other (as in configuring communications software to work with a modem).

Copyright: all rights of copyright whether existing now or in future, in or to the Ministry of Finance IT Resources.

Crash: A problem (often caused by a bug) that causes a program, or the entire operating system, to unexpectedly stop working.

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.

Data Owner: the Ministry of Finance User or Department authorized by the Ministry of Finance Management to permit access to information or data and that is responsible, on behalf of the Ministry, for the integrity and accuracy of that information or data.

Driver: A piece of software that tells the computer how to operate an external device, such as a printer, hard disk, CD-ROM drive, or scanner.

E-mail: Electronic Mail. Private messages sent between users on different computers, either over a network or via a modem connection to an on-line service

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.

File Server: A computer that shares its resources, such as printers and files, with other computers on the network. An example of this is a Novell NetWare Server which shares its disk space with a workstation that does not have a disk drive of its own.

Firewall: A mechanism that isolates a network from the rest of the Internet, permitting only specific traffic to pass in and out.

Hardware: all physical Components, which make up, either singly or collectively, a device that can be used for data processing. This includes, but is not limited to, not only the computer proper but also the cables, connectors, power supply units, and peripheral devices such as the keyboard, mouse, audio speakers, and printers

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.

IP Address: Network addresses are usually of two types: (1) the physical or hardware address of a network interface card; for Ethernet this 48-bit address might be 0260.8C00.7666. The hardware address is used to forward packets within a physical network. (2) The logical or IP Address is used to facilitate moving data between physical networks and is made up of a network number, a sub-network number, and a host number. All Internet addresses at SDSU have a network number of 130.191, a subnet number in the range of 1-254, and a host number in the range of 1-254.

ISP: Internet Service Provider is a company that provides access to the Internet. A service provider can offer simple dial-up access, SLIP/PPP access, or a dedicated line.

Login: The account name used to access a computer system.

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

Memory: In general, another word for dynamic RAM (Random Access Memory), the chips where the computers store system software, programs, and data you are currently using. Other kinds of computer memory you may encounter are parameter RAM (PRAM), video RAM (VRAM), and static RAM (SRAM). Most computer memory is volatile, that is, its contents are lost when the computer shuts down.

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.

Motherboard: The heart, soul, and brains of a computer. This plastic board resembles a miniature city, but its buildings are actually chips for things like the processing RAM, and ROM, and the tiny roads connecting them are circuit traces; also called the logic board.

Multimedia: Any presentation or software program that combines several media, such as graphics, sound, video, animation, and/or text.

Network: In general, a group of computers set up to communicate with one another. Your network can be a small system that's physically connected by cables (a LAN), or you can connect separate networks together to form larger networks (called WANs). The Internet, for example, is made up of thousands of individual networks. A group of computers, Peripherals and electronic Components that share information and applications electronically, typically connected to each other by either cable and / or telecommunication links.

Patch: A is a piece of software designed to fix problems

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.

Regression Testing: The selective retesting of a software system that has been modified to ensure that any bugs have been fixed and that no other previously working functions have failed as a result of the reparations and that newly added features have not created problems with previous versions of the software.

Router: A special purpose computer that attaches to two or more networks and routes packets from one network to the other. A router uses network layer addresses *(such as IP Addresses)* to determine if packets should be sent from one network to another. Routers send packets to other routers until they arrive at their final destination

Server: A computer that shares its resources, such as printers and files, with other computers on the network. An example of this is a Novell NetWare Server which shares its disk space with a workstation that does not have a disk drive of its own.

Software: shall mean all computer programs and the customization thereof, identified or developed by or on behalf of Ministry of Finance, also including the compiled object code of such programs and the customization of adapted Software packages.

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

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

System Administrator: shall mean an employee of Ministry of Finance, whose responsibilities include System, site, or network administration for Ministry of Finance Systems. A System Administrator's functions include, inter alias, installing hardware and Software, managing a computer, network or application, and keeping Ministry of Finance Systems operational.

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

UPS: Uninterruptible Power Supply; a unit that switches to battery power whenever the power cuts out.

User: shall mean a User with authorization to access Ministry of Finance systems or networks, but without System Administrator privileges and responsibilities for the Ministry of Finance Systems or networks.

User Id: The string of characters that identifies the user on the system and will ensure access in addition to the password; this the name by which the user is known to the network; also known as username.

Virus: A program that replicates itself from one file or disk to another without your consent. They are spread through floppy disks, networks, and on-line services and can go undetected (unless you have an antiviral utility) until something goes wrong. Some viruses deliberately destroy data, and even those designed to be benign can cause crashes, slowdowns, and file corruption.

Wide Area Network (WAN): Network spanning multiple geographic distances, usually connected by telephone lines, microwave, or satellite links.

WWW: World Wide Web or W3 is the hypermedia document presentation system that can be accessed over the Internet using software called a Web browser.

Zipped: Compressed version of a program or document.

1. INTRODUCTION

1.1 Background

Information Communication Technology (ICT) has taken the world by storm resulting not only in benefits for the individual but also for corporations, the Ministry of Finance under the direction of the Government of the Republic of Namibia took advantage of this advancement and benefits of ICT to develop and implement several ICT systems for effective and efficient service delivery; both for itself and also for its sister ministries.

The Ministry has invested in the development of shared ICT infrastructure consisting of various structured networked technologies to most of its buildings located at the Head Office and remote offices including other ministries and organizations. Also, the Ministry has invested in various software technologies such as the IFMS, ASYCUDA System, Tax System, Office Application, to mention but a few; which enable communication and collaboration between various entities.

MOF is committed to use ICT to ensure effective and efficient service delivery to the public as well as to ease the work of its staff members. The Ministry acknowledges the need to implement measure to address and protect itself from many security challenges brought by the technology advancement. To address information security issues, the Ministry of Finance has developed various security documents (standards, procedures and policies) which provide guidance in the proper usage, management and administration of all ICT resources.

1.2 Purpose

The main purpose of this policy is to provide guidelines and a framework for selecting, implementing, and managing ICT security services by guiding the organization on how to manage ICT assets such as, but not limited to, computer hardware, printers, data, Networks, long-distance data services, software applications and any other current or future Information Technology Resources adopted, acquired, installed, deployed or operated by the Ministry of Finance.

Moreover, the policy intends to protect both the data stored and processed within the ministerial systems together with the services provided by these systems for the purpose of protecting information confidentiality, integrity and availability; and ultimately creating a unified

environment of handling ICT security issues for both MOF staff and external parties who access MOF's ICT resources.

This policy document provides guidance on issues relating to the development of agreements that define the service levels for service providers; as well as an understanding of security issues for the purpose of deciding on comprehensive ICT security services.

1.3 Scope

This Policy applies to all Ministry of Finance employees, consultants and any other party who uses MOF ICT resources in any form. 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

This Policy is a living document which implies that it will be under constant review and amendment to ensure that it is aligned to address new technological challenges and business practices.

Suggestions, questions and concerns are welcome, and should be addressed in writing to:

Deputy Director
Information Technology Division
Ministry of Finance

1.4 Disclaimer

This policy document is expected to provide guidance on the proper use of ICT facilities in MoF, it is not by any way exhaustive (this is a living document) 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 resources 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 and the use of this equipment must be understood by the staff members.
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 ITD 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 ITD will ensure the implementation of the above measures.

2.2 Measures against Floods (Water)

i. Servers should be well mounted on racks and other equipment should be kept off the ground, placed on tables or desks.
ii. The office shall take precautions to prevent the ingress of water, or any other damaging

fluid substances into the area of computer operation.

iii. Windows in the vicinity of computers shall be kept closed when in is raining.
iv. Ensure that roofs are sealed properly, to prevent the leaking of water in areas of computer equipment.
v. Leaking of water shall immediately be reported to Administration.
vi. Clear flood instructions should be available and in the event of flood, these instructions should be followed.
vii. 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 ITD 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 a conducive environment for the ICT equipment.
ii. The air conditioners should be serviced regularly to ensure continuous performance and be documented.
iii. Air conditioning failure should be reported for immediate remedial measures.

The Head of the ITD will be responsible for the air conditioning measures.

2.4 Power Outage

ICT assets can be adversely affected by reduction or increase in the voltage or frequency of power supplies and therefore measures need to be put in place to prevent this.

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. All computers shall be protected by surge suppressing power supplies (clean power lines, e.g. red plugs for computer hardware only).
v. A generator of appropriate capacity should be serviceable at all times as backup power supply in the event of power outage.
vi. Darkness can seriously disrupt plans for dealing with emergencies. The building owners are responsible to provide backup lighting for dealing with emergencies.

The Head of Administration and Human Resource Department in collaboration with the ITD 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 in collaboration with the ITD 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 as well as all protection of physical ICT resources (computers, printers, etc.). This is categorized into two areas namely Physical Access and Logical Access.

3.1 PHYSICAL ACCESS CONTROL

Protection of the physical ICT resources including access to the Server room, Disaster Recovery Site and Computer rooms should base on the following requirements and all staff should be trained on how to observe access procedures

3.1.1 Entrance Doors

i. All entrance doors to the different floors will be fit with an access control card reader and a magnetic door lock to allow access to authorised personnel only.
ii. All doors will be fit with a hinge on the door to ensure that all entrance doors are always closed.
iii. All doors will be fit with door contact to indicate via an alarm on the alarm system when these doors are open.
iv. CCTV should be located in strategic positions within specific areas in various places,
v. Each staff member will be allocated an access control tag that will be configured on the alarm system.
vi. 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.
vii. Should a tag get lost, the staff member should report it to the Administration directorate immediately to deactivate such a tag. A replacement tag will be issued

3.1.2 Server Room, Computer Equipment Safes and Strong Rooms

i. Access to the server room, computer equipment safe and strong rooms is restricted to only authorised ITD personnel and keys to access these areas should be kept in a secure place.
ii. Other Staff members within MoF and contractors requiring access to the Server room

must notify the ITD through the Deputy Director.

iii. Other Staff/Visitors authorized to enter the Server and Computer rooms should be accompanied by designated officer of the ITD and should be logged in the register book

iv. CCTV is required in these rooms and an intruder alarm system should be installed at the entrance to these rooms.

3.2 LOGICAL ACCESS CONTROL

Protection of the logical access to ICT resources should base on the following requirements and all staff should be trained on how to observe access procedures

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 formally request access by means of an official letter signed by the relevant authority clearly indicating the access privileges for the application/system in question.

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 Administrators 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 the network will be by individual username and password
ii. Access to resources on the systems network should be restricted unless specifically authorized.
iii. Users are expressly forbidden from making unauthorized alterations or extensions to the network.
iv. A register of network device, their access restrictions and the protocols in use should be kept by the Network Administrator.
v. All changes to network configurations should be recorded in the register, along with authorization for the changes.
vi. Users should be permitted to use only those network addresses issued to them by the relevant authority.
vii. 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.
viii. 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.
ix. 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.
x. Network devices and traffic should be monitored regularly.
xi. Results/Logs from the firewall should be reviewed by ICT Security Officer to confirm there have been no unexpected attempts to connect.
xii. 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.
xiii. Users should not install network hardware or software that provides network services without being approved.
xiv. Computers that require network connectivity should conform to systems standards.
xv. Users with administrative privileges 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.
xvi. Users are not permitted to alter network hardware in any way.

xvii. Access to network will be restricted to normal working hours during weekdays for staff members below middle management level, unless otherwise authorised.

3.2.3 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. Disclosure of passwords is prohibited; and passwords should be hard to guess but easy to remember.
iii. Passwords must be unique and have no relationship to information connected to the user, e.g. names of family members.
iv. Passwords will expire every 90 days and the last three (3) passwords cannot be reused.
v. The user account will be locked after incorrect attempts
vi. The ITD shall be notified by the Personnel Division of all new employees and all employees leaving the office's employment. The ITD will disable the account of a user that has resigned, on his/her last working day and no later than 3 weeks from the date of last working day.
vii. Paper based records of passwords of systems super user (e.g. server, network, database passwords) should be placed in a sealed envelope, signed by two authorized persons across the seal, and keep it in a locked, fireproof safe. These passwords can only be accessed through the Deputy Director of the ITD.
viii. Passwords should be changed the moment that a breach of confidentiality is suspected.

3.2.4 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 ITD for investigation.
ii. Remote User accessing MoF systems should be authenticated by remote access server.
iii. Where the network is accessed remotely via wireless appropriate wireless security

standards will be used. Wired Equivalency Protocol (WEP) and a WEP key will be used as standard on Wi-Fi connections and Wi-Fi Protected Access (WPA) will be used where it is available.

iv. Access from remote users to the corporate network will be via secure IPSEC VPN or SSL VPN connections only. This is necessary to secure the connection from the remote device to the corporate network.

v. To prevent remote PC's, laptops or other mobile devices. from compromising the corporate network, security software will be installed on the devices.

vi. Devices that are used to access the network remotely, must meet the minimum standard for supported web browsers and operating systems that is current at the time of access. Where access is provided directly to the corporate network, users will only be allowed access on standard devices authorised and approved by ITD.

3.2.5 Clear Screen

All users of workstations, PCs and laptops with access to the various applications and system hosted by the MOF; 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 required to regain access to the screen.

3.2.6 Logon and Logoff from Computer

To avoid Information Security breaches, users should lock or log off their computers while they are not in use. 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 and should report the inability of users to log on, to the designated Information Security Officer.

vii. Designated Systems Administrator should double check that users have logged off at the end of the working day.

viii. Users should ensure that they log off computer workstation before leaving their desk.

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

4. DATA AND INFORMATION SECURITY

The protection of data and information is critical to the existence and persistence or any organisation and this also applies to the Ministry of Finance. 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.

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 (i.e. the C drive on the personal computer or on mobile devices (e.g. laptops), 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 be 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 asstipulated 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.

Head of the ITD will be responsible for security of transfer and exchange of information.

4.3 SECURITY OF MEDIA IN TRANSIT

Information can be vulnerable to unauthorized access, misuse or corruption during physical transportation, 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 ITD 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 of 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 ITD 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 be based 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 Policy. These designated system developers should not be permitted to access the live system and its database.
ii. Safe and secure copy of the data should be provided, once the terms of use have been authorized.
iii. Development and testing work should be isolated from normal processing work by means of separate machines or partitions.
iv. The techniques used to capture the live data should not permit subsequent or additional access to the live system by the designated system developers.
v. 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.
vi. Test files and printouts that contain copies of live data should be properly disposed of and effectively destroyed after use.

The head of the ITD 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, through the form of 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 systems 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 ITD 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. The 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. The designated System Administrator should regularly search for rogue or unauthorized wireless access points;
iv. Once a device is reported missing, the 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. Deploy secure wireless technologies on top of wireless network.
vii. 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, tablets, etc.) that are used outside network boundary. Turn off sharing at wireless clients.

ii. 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.
iii. Enable wireless connections only when users need them and disable them when they are no longer in use.
iv. Follow the guideline protection against computer virus and malicious code.

The head of the ITD 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. ITD 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 ITD 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 also bound to this guideline.

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

5.4 E-MAIL SECURITY

Electronic Mail (E-mail) communication is very efficient and cost effective at communicating in written and multimedia form. The Email creates a means to communicate with more than one person at the same time from anywhere in the world; this ease of use makes email communication open to abuse, thus advancing illegal and unlawful actions including the

transmission of various computer virus.

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 and exposing 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.

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 ITD will be responsible to ensure the adherence of the guidelines for protection against cyber-attacks.

5.6 PROTECTION AGAINST COMPUTER VIRUSES AND MALICIOUS CODE

A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other files; when this replication succeeds, the affected files are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes.

Computer viruses currently cause billions of dollars' worth of economic damage each year, due to causing systems failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. Therefore protection against Computer viruses and malicious code should be done based on the following requirements:

i. The designated MoF System Administrator should enable real-time detection to scan computer virus and malicious code for active processes, executable and document files that are being processed.
ii. The 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. The 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, the 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 files 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. The designated MoF System Administrator should conduct daily update of the virus definition files to minimize the risk of infection from new viruses.
viii. The 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 must 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 the 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 ITD 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 will be 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 ITD to ensure conformity to predefined standards.

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

6.1 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, and such tests should be documented, so that the logical errors are rectified accordingly.

6.2 SOFTWARE ACQUISITION

i. On acquiring software, proper procurement procedures should be followed as stated in the Tender Board 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 ITD should ensure proper management of licenses for the software acquired.

vi. Acquired critical software should be covered by an agreement (i.e. Escrow agreement) to ensure continuity.

vii. Use of open source software should adhere to the Government Circular <circular # and

date> of Permanent Secretary OPM.

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

6.3 SOFTWARE DEPLOYMENT

Software deployment is all of the activities that make a software system available for use and involves the installation and testing of software, amongst others.

The general deployment process consists of several interrelated activities with possible transitions between them.

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; this 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; and installation should be done properly.
v. Any deployment of software in MoF environment should be approved by relevant authority.

6.4 SOFTWARE CUSTOMIZATION

i. All software customizations should comply with user department requirements and MoF security guidelines.
ii. Software customization should adhere to the guidelines under the Software Development and Deployment, mentioned above.
iii. Designated officer should verify that need for a particular customization has been met.

6.5 SOFTWARE USAGE

i. Software should be used for the intended purpose as stipulated in the terms and conditions of the software.
ii. Before an employee is permitted to use the particular software, the designated

department should instruct users on the proper usage of the particular program.

iii. The designated department should inform users on terms and conditions included in the license agreement accompanied by the program.

6.6 SYSTEMS INTEGRATION AND INTEROPERABILITY

System integration is defined as the process of bringing together the component subsystems into one system and ensuring that the subsystems function together as a single system. In information technology, systems integration is the process of linking together different computing systems and software applications physically or functionally, to act as a coordinated whole. Interoperability is the ability of diverse systems and organizations to work together (inter-operate). With respect to software, the term interoperability is used to describe the capability of different programs to exchange data via a common set of exchange formats.

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.

6.7 SOFTWARE CHANGE MANAGEMENT

Software Change Management is the process of planning, organizing, controlling, executing and monitoring changes that affect the delivery of ICT services in its entirety.

It encompasses all components and activities required to direct additions, modifications and deletions. Software change request should be submitted for approval using the Change Request Form (Appendix B).

6.7.1 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 if based on the following requirements:

i. All staff involved in installing the new software or upgrade should be suitably qualified, trained and supervised.
ii. A suitable contingency plan should be in place in case of failure of the new software.

iii. The Systems Administrator should properly test new or upgraded software before deploying it in a live environment; based on the approved pre-designed test plan.
iv. Upgraded software versions should offer at least the current level of security safeguards.
v. The system owner(s) 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 and not just those which have been changed or updated.
vii. The system owner(s) 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.

6.7.2 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. The system administrator should verify that the patches are necessary and come from an authorized source, normally the software manufacturer or vendors.
iii. The system administrator should ensure that updates to the system documentation are received with the patches.

6.7.3 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 have been analyzed. 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 the 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.

6.7.4 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 be 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.

6.7.5 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.

6.7.6 Emergency Change Request

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.

The head of the ITD will be responsible to ensure the guidelines for software development, acquisition, deployment, customization and usage as well as systems integration and interoperability and software change management are adhered to.

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 Evaluation

The Information system security officer should evaluate risks based on magnitude and impact of risks for example, low, moderate, high, and extreme.

7.1.3 Risk Assessment

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

i. The Information security officer should be aware of Organization objectives and assess risks in collaboration with these objectives.
ii. The Information security officer should prepare an Information Systems Risk Inventory, clearly indicating the actual impact of the identified risks. 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.

7.1.4 Risk Treatment

The Information system security officer should develop a feasible and cost effective risk treatment strategy. This treatment should be clearly documented and updated on a regular basis

7.1.5 Risk Monitoring and Review

Whatever the risk treatment option selected, the 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. The Information Security officer should have appropriate tools to track, identify and document security breach incidents.

7.3 DISASTER RECOVERY PLANNING

A disaster recovery plan, which includes a Back-up plan, should be put in place for MoF's valuable data. The 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. The DRS team should be trained and assigned the task of maintaining and executing the Disaster Recovery Plan.

The MoF Disaster Recovery Plan should constitute of the following:

i. The Information system security officer should recommend a data backup and business continuity solution.
ii. The Information system security officer should align and communicate the Ministry data back-up and disaster recovery planning policies to user departments.
iii. Copies of the MoF databases should be in near real time backed up onto the DRS servers.
iv. The Database Administrator should backup all critical systems to the offsite as per Disaster Recovery Plan.
v. The System owner(s) 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; as part of continuity.
x. Ensure the 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 ITD.

The head of the ITD in collaboration with the Head of Administration will be responsible to

ensure the guidelines for Business Continuity Management are adhered to.

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 the 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 A)
iv. In case a Third party needs to access MoF systems they should be assigned new logon details (username and passwords) and relevant access privileges.
v. Any created user logon details to allow access to MoF systems, should be changed as soon as access is no longer required.

The head of the ITD will be responsible for the implement the above guidelines.

8.2 OUTSOURCING

Prior to entering into an ICT outsourcing arrangement, care should be taken to ensure that this process will not compromise the Organization's objectives, policies and standards. Thus, the 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 should be in place.

vi. Compliance with information, security and privacy policies, laws and regulations should be adhered to at all times.

vii. Access Protocols and remote access controls should be met by the provider, its staff and contractors, and monitored by the ITD.

The head of the ITD will be responsible for the implement 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. Cryptographic mechanisms should be used to ensure the authentication, integrity and confidentiality of data and communications involved.

iv. Examine if the cloud computing vendor is a "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 cryptography 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, unless otherwise stated in the agreement. 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 ensure protection 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 ITD 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 sensitivity of data, the ITD 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 ITD 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 the right to have information system audit conducted (internal or external).

8.6 INTERNET SERVICE PROVIDER

i. The ISP should in writing 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 CRAN standards.

8.7 THIRD PARTY CONTRACT MANAGEMENT

A 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 them obtaining access to the systems and information.

9.1 SECURITY TRAINING TO MOF USERS

To give appropriate security training to MoF users, the users have been categorized into technical users, end-users and temporary employees/trainees. All new staff members should be trained on the security aspects of all the current ICT resources as well as the newly procured ICT resources

9.1.1 Technical User

i. Technical users should be trained on security aspects for newly procured software and hardware.
ii. Regular training should be conducted to technical users; this includes systems analysts, system administrators and Information Security officers on the use of patches for existing software.
iii. The Information System Security officer should monitor and review the level of information security knowledge of technical and operation staff on a 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 newly 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. Be attached to a selected location and be 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 ITD.
ii. Users of ICT resources should be trained and provided with copies of ICT Security Policy 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 and 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 ITD 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 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. 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 assigned 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 of a new employee to ITD 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 ITD 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. Where possible, the account of employees who are on leave 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 the HR department and ITD during termination process:

i. Human Resource officer should provide information, on regular basis, to the ITD concerning employees who are leaving the organization.
ii. The system administrator should ensure that the system account for the 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 Policy. In a scenario whereby the ICT activities within MoF appears to be not in line with this Policy, this tool will help to get ICT operations back on the right track.

The 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 policy so as to take on board new security changes.

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

i. Oversee all information on security issues at the Ministry of Finance.
ii. Monitor regularly these policy guidelines to ensure that all users are adhering to them.
iii. Distribute and interpret the ICT Security Policy guidelines as depicted in this document to MoF employees and third party entities.
iv. Provide feedback to ICT Steering Committee on the issues, obstacles, challenges and achievements made during implementation of the policy.
v. In addition, monthly, quarterly, biannual and annual reports will be prepared for the ICT Steering Committee to brief them on various issues relating with ICT security.

13. REFERENCES

14. APPENDIX A: CONFIDENTIALITY & COMPLIANCE AGREEMENT FORMS

MINISTRY OF FINANCE: REPUBLIC OF NAMIBIA

CONFIDENTIALITY AND ICT SECURITY COMPLIANCE – NON-EMPLOYEE

The Ministry of Finance (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 Policy.

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

1. That I have carefully read and understood the contents of the "ICT Security Policy", 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 and 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 Policy guidelines, stern legal measures shall be taken against me.

Name: _____

Date: _____

Signature: _____

Company Details: _____

_____

……

FOR OFFICIAL USE ONLY: Endorsed By:

Name: _____

Position: _____

Signature: _____

Date: _____

MINISTRY OF FINANCE: REPUBLIC OF NAMIBIA

CONFIDENTIALITY AND ICT SECURITY COMPLIANCE – EMPLOYEE

The Ministry of Finance (MoF) regards security and confidentiality of data and information to be of utmost importance. Each employee 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 Policy.

I, _____

(Print full first, middle & surname – block letters and in ink) Note: Use of the full name is important. It must match personnel records in the HR Department. Do not use abbreviated or nicknames (e.g. Shelley for Michelle, Meg for Margaret, etc.) unless it is your formal name.

Hereby solemnly state as follows:-

1. That I have carefully read and understood the contents of the "ICT Security Policy", copies of which were supplied to me by the ICT Unit/MoF Management and agree to abide by the guidelines stipulated herein.

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 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.

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

Name: _____

Employee #: _____

Position: _____

Division: _____

Date: _____

Signature: _____

……

FOR OFFICIAL USE ONLY: Endorsed By:

Name: _____

Position: _____

Signature: _____

Date: _____

15. APPENDIX B: CHANGE REQUEST FORM