Ministry of Finance – Information Technology Division

Standards and Guidelines for Computing and Networking Facilities

Version 0.1

Table of Content

1. Conditions of use of computing and network facilities

It is the policy of the Ministry of Finance that the computing and network facilities are intended for the use to support the mission, vision and core objectives of the MoF as stipulated in the Constitution of the Republic of Namibia and in the strategic plans of the Ministry of Finance.

All persons using the computing and networking facilities shall be responsible for the appropriate use of the facilities provided as specified by the "Codes of Practice" of this document and shall observe all conditions as published by the Systems Administrator.

It is the policy of the Ministry of Finance that the computing and associated network facilities are not to be used for commercial purposes or non-MOF related activities without written authorization from the Permanent Secretary.

The Ministry of Finance will endeavour to protect the confidentiality of information and material furnished by the user and will instruct all computing personnel to protect the confidentiality of such information and material, but the Ministry of Finance shall be under no liability in the event of any improper disclosure

The Ministry of Finance will endeavour to safeguard the possibility of loss of information within the MoF's computing and networking facilities but will not be liable to the user in the event of any such loss. The user must take all reasonable measures to further safeguard against any loss of information within the MoF's computing and networking facilities.

If the loss of information within the system can be shown to be due to negligence on the part of the computing and networking personnel employed by the Ministry of Finance, or to any hardware or software failure which is beyond the user's means to avoid or control; then the Information Technology Division will endeavour to help restore the information.

Users of the computing and networking facilities recognize that when they cease to be formally associated with the Ministry of Finance (E.g. No longer an employee) their information may be removed from the Ministry of Finance computing and networking facilities without notice. Users must remove their information or make arrangements for its retention prior to leaving the Ministry of Finance.

The Deputy Director of Information Technology Division may suspend any person from using the computing and networking facilities for a period not exceeding 30 days (or may recommend additional penalties to the Permanent Secretary) if after appropriate investigation that person is found to be

1.1 Responsible for wilful physical damage to any of the computing and networking facilities
1.2 In possession of confidential information obtained improperly
1.3 Responsible for wilful destruction of information
1.4 Responsible for deliberate interruption of normal services provided by the IT Division
1.5 Gaining or attempting to gain unauthorized access to accounts and passwords
1.6 Gaining or attempting to gain access to restricted areas without the permission of the Deputy Director
1.7 Responsible for inappropriate use of the facilities.

2. Code of Practice in the use of computing and network facilities

2.1 Introduction

Standards for the use of the computing and networking facilities of the Ministry of Finance is derived from standards of common sense an common decency that apply to the use of any shared resources.

The purpose of the Code of Practice is to specify user responsibilities and to promote the appropriate use of Information Technology for the protection of all members of the Ministry of Finance.

2.2 Appropriate and reasonable use

Appropriate and reasonable use is defined as use that is consistent with the objectives, mission and vision of the Ministry of Finance. All uses inconsistent with these objectives are considered to be inappropriate use.

Users of the Ministry of Finance computing and network facilities accept the following responsibilities:

2.2.1 To safeguard their data, personal information, passwords and authorization codes and confidential data

2.2.2 To choose passwords wisely and to change them periodically

2.2.3 To take full advantage of file security mechanisms built into the computing systems

2.2.4 To follow the security policies and procedures established to control access to and use of administrative data.

2.2.5 Not to divulge sensitive personal data to which they have access to; respecting the privacy of other users and not to represent others, unless authorised to do so explicitly by those users

2.2.6 To respect the intended usage of system for electronic exchange (e.g. Email, World Wide Web, etc); for example, not to send forged electronic mail, mail that will intimidate or harass other users, chain messages, mass-mail, social networks; that can interferer with the efficiency of the system, accessing and reading another user's electronic mail without their permission.

2.2.7 To respect the integrity of the computing and networking facilities; for example, not to intentionally develop or use programs, transactions, data or processes that harass other users or infiltrate the system or damage or alter the software or data components of a system. Alterations to any system or network software or data components are to be made only under specific instructions from persons in authority.

2.2.8 To adhere to all general policies and procedures of the Ministry of Finance, including but not limited to the policies on proper use of information resources and computing and networking facilities; the acquisition, use and disposal of MoF-owned computer equipment, use of telecommunications equipment; legal use of software and legal use of all data.

2.2.9 To report any information concerning instances in which the Ministry of Finance IT Security Policy or any of its standards/guidelines and codes of conduct has been or is being violated. Reports about such violations should be channelled to the head of department/division or directly to the Deputy Director of the IT Division.

2.3 Specific Activities' code of practice

The following apply to specific activities

2.3.1 Illegal Activities

In general, it is inappropriate use to store and/or give access to information on the Ministry of Finance computing and networking facilities that could result in legal action against the Ministry.

2.3.2 Restricted Hardware and Software

User should not knowingly possess, give to another person, install on any of the computing and networking facilities, or run, programs or other information which could result in the violation of any the Ministry of Finance policy or the violation of any applicable license or contract. This is directed towards but not limited to software known as viruses, Trojan horses, worms, password breakers and packet observers. Authorization to possess and use Trojan horses, worms, viruses and password breakers for legitimate diagnostic purposes can be obtained from the Deputy Director of Information Technology Division.

The unauthorised physical connection of monitoring devices to the computing and networking facilities which could result in the violation of the Ministry's policy or applicable licenses or contracts is inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and networking facilities for the purpose of monitoring data, packets, signals or other information. Authorisation to possess and use such hardware for legitimate diagnostic purposes must be obtained from the Deputy Director of Information Technology Division.

2.3.3 Harassment

The Ministry of Finance policy and the Government of the Republic of Namibia prohibits sexual and discriminatory harassment; therefore the computing and networking facilities of the MoF are not to be used to tarnish, slander or harass any other person.

The following constitute examples of Computer Harassment:

2.3.3.1 Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family.

2.3.3.2 Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.

2.3.3.3 Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he/she desires such communication to cease.

2.3.3.4 Intentionally using the computer to invade the privacy of another or the threatened invasion of the privacy of another.

2.3.4 Wasting Resources

It is inappropriate use to deliberately perform any act which will impair the operation of any part of the computing and networking facilities or deny access by legitimate users to any part of them. This includes but is not limited to wasting resources, tampering with components or reducing the operational readiness of the facilities.

Wastefulness includes but is not limited to passing chain letters, wilful generation of large volumes of unnecessary printed output or disk space, wilful creation of unnecessary multiple jobs or processes, or wilful creation of heavy network traffic.

2.3.5 Game Playing

The computing and networking facilities of the Ministry of Finance are not be used for game playing.

2.3.6 Commercial use or use for Personal Business

The Ministry of Finance computing and networking facilities are provided by the Ministry for the support of its mission; therefore it is inappropriate to these facilities for commercial gain or placing a third party in a position of commercial advantage.

The computing and networking facilities may not be used in connection with compensated outside work.

2.3.7 Connection to the data network

To maintain the integrity of the Ministry of Finance computing and network facilities, connections to the campus network are made only by specialised personnel under the direction of the Information Technology Division.

Users are encouraged to attach appropriate equipment only at existing user-connection points. All requests for additional network connections or for the relocation of a connection should be directed to the head of networking in the Information Technology Division.

2.3.8 Use of Desktop Systems

Each user is responsible for the security and integrity of the Ministry of Finance information stored on their personal desktop system from wherever they are working. This responsibility includes making regular disk backups, controlling physical and network access to the machine, and installing required operating system patches and using appropriate virus protection software.

Users should avoid storing passwords or other information that can be used to gain access to other computing resources. Do not store Ministry passwords or any other confidential data or information on laptops or home PCs or associated disks. All such information should be secured after any dialup connection to the MoF network.

2.3.9 Printouts

Users are responsible for the security and privacy of printouts of the Ministry of Finance information.

3. Appropriate use of the Electronic Mail (E-mail)

3.1 Introduction & Scope

Electronic mail and communication facilities provided by the Ministry of Finance are intended to ease the communication process whilst implementing the core business of the ministry. The use of the Electronic mail and communication facilities are governed by the rules and policies of MoF and applicable laws; as well as acceptable use policy of the provider.

Electronic mail may be used for personal communications within appropriate limits.

These standards of use cover all electronic mail systems used by members of the Ministry of Finance community (this includes third parties), from the MoF network or when connecting to the MoF network or while acting in an official MoF capacity.

3.2 Appropriate use and responsibility of users

Electronic mail can be both informal like a phone call and yet irrevocable like an official memorandum; due to this, users should explicitly recognize their responsibility of the content, dissemination and management of the messages they send.

This responsibility means ensuring that messages:

3.2.1 Do not contain information that is harmful the Ministry of Finance or member of the Ministry of Finance community
3.2.2 Are courteous and polite
3.2.3 Are not for commercial purpose unless authorized by the Ministry of Finance
3.2.4 Are consistent with MoF policies

3.2.5 Protect others' right to privacy and confidentiality
3.2.6 Do not contain obscene, offensive or slanderous material
3.2.7 Are not used for purposes that conflict with MoF interests
3.2.8 Contain an accurate, appropriate and informative signature.
3.2.9 Do not unnecessarily or frivolously overload the email system (e.g. spamming unnecessary forwards and junk mail is not allowed)

An appropriate "Out of Office" message, for your E-mail, should be activated for users who are absent from work for two or more days. This message should indicate who should be contact during your absence to ensure that continued service is provided.

Electronic mail that contains a formal approval, authorization, delegation or handing over of responsibility must be copied to paper and filed appropriately for purposes of evidence and accountability.

3.3 Data backups

Although the Information Technology Division does everything possible to back up data stored on central server areas, it is the responsibility of the individual user to backup their own data from their computers, safely onto tape, diskette or other media. It is the responsibility of the individual to store all information that is of value to the Ministry of Finance on a recommended server supplied by the MoF.

3.4 Confidentiality and Security

1. Electronic mail is inherently NOT SECURE
2. As the networks and computers are the property of the Ministry of Finance, the MoF retains the right to allow authorized MoF officers to monitor and examine the information stored within.
3. It is recommended that personal confidential material not be stored on or sent through the MoF equipment
4. Users must ensure the integrity of their password and abide by MoF policy on password security. (See the section on Password Security)
5. Sensitive confidential material should NOT be sent through the electronic mail system unless it is encrypted.
6. Confidential information should be redirected only where there is a need and with the permission of the originator.
7. Users should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies.
8. Electronic mail messages can be forged in the same way as faxes and memoranda. If a message is suspect, users should verify its authenticity via telephone.

3.5 Use Indemnity

Users **agree** to indemnify the Ministry of Finance for any loss or damage arising out of improper use.

3.6 Limited Warranty

The Ministry of Finance takes no responsibility and provides no warranty against the non-delivery or loss of any files, messages or data nor does it accept any liability for consequential loss in the event of improper use or any other circumstances.

4. Guidelines on passwords

4.1 Password management:

4.1.1 Passwords should be memorize – never written down

4.1.2 Passwords belong to individuals and must never be shared with anyone else (unless it's a group password, where only those in the group need to know the password)

4.1.3 Passwords should be changed every month, or immediately if compromised.

4.2 Password Administration

4.2.1 System Administrators should regularly run password cracking software against their password files to identify weak passwords

4.2.2 New or changed passwords must be given in writing only to the identified user – never over the telephone or via email.

4.3 Password Construction

Password security isn't just a matter of thinking up a nice word and keeping it to yourself. You must choose a password the will be difficult to guess or crack. The following are guidelines on choosing a password.

4.3.1 A password should be at least 6 characters long

4.3.2 NEVER make your password a name or something familiar, like your pet, your children, partner, favourite actor/actress or food; these are also guessable.

4.3.3 NEVER, under any circumstances, should your password be the same as your username or your real name

4.3.4 DO NOT use words that can be associated with you

4.3.5 DO NOT use dictionary words as a password. Most basic cracking programs contain 80000 words and plenty of variations

4.3.6 Try to have a password with a number or missed case letter. Simple substitutions like '1' or an 'l', and '0' of an 'o' are easily guessed. Make use of special characters as this strengthens the password. Add a '%' or '$ to the middle of the password.

4.3.7 Choose something you can remember, that can be typed quickly and accurately and includes characters other than lowercase letters.

5. Internet conditions, standards and guidelines

5.1 Introduction and Scope

New risks and opportunities are introduced by the resources, services and inter-connectivity provided on the internet; in response to the risks, this statement describes the Ministry of Finance official policy on Internet Security.

These standards and guidelines apply to all Ministry of Finance employees and third parties who use the internet with the Ministry of Finance computing and networking resources, as well as those who represent themselves as being connected to the Ministry of Finance.

5.2 Transmission of Information

5.2.1 Downloading

All software downloaded from non-Ministry of Finance sources via the Internet must be screened with virus detection software prior to being installed. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine. If this software contains a worm, virus or Trojan horse, then the damage will be restricted to the involved machine.

5.2.2 Contacts

Contacts made over the Internet should not be trusted with Ministry of Finance information unless reasonable steps have been taken to ensure the legitimacy of the contacts. This applies to the release of any internal MoF information

5.2.3 Information Security

Wiretapping and message interception is straightforward and frequently encountered on the internet. Therefore, Ministry of Finance, proprietary or private information must not be sent over the Internet unless it is encrypted by approved methods. Log-in passwords and other parameters that can be used to gain access to MoF systems, networks and services, must not be sent over the Internet in readable form.

5.2.4 Suspected Information

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

5.3 Software Security

Ministry of Finance computer software, documentation, and all other types of internal information must not be transferred to any non-MoF party for any purpose other than MoF purposes expressly authorized by Permanent Secretary or the Minister.

Exchange of software and/or data between MoF and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

The Ministry of Finance strongly supports strict adherence to software vendors' license agreement and it is subject to random audits by these vendors. When MoF computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

5.4 Personnel Security

5.4.1 Privacy

Staff using the Ministry's information system and/or Internet should realise that their communications are not automatically protected from viewing by third parties. If encryption is not used, workers should not send information over the Internet if they consider it private.
Any doubt regarding the privacy of information should be resolved by contacting the Director of the Directorate where the information origination or the Information Technology Division.

5.4.2 Right to Examine

At any time and without prior notice, the Ministry of Finance management reserves the right to examine e-mail, personal file directories, and other information stored on MoF computers. This examination assures compliance with internal policies, supports the performance of internal investigations and assists with the management of MoF information systems.

5.4.3 Resource Usage

The Ministry of Finance encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not MoF time. Likewise all non-MoF activities (games, news groups, etc) must be performed on personal not MoF time.
Use of the MoF computing and networking resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no MoF activity is pre-empted by personal use.

5.4.4 Public Representation

Staff may include their affiliation with the Ministry of Finance in public forums (including the Internet discussions), however they must make it clear that opinions expressed are their own, and not necessarily those of the Ministry of Finance.

All external representations on behalf of the Ministry of Finance must first be cleared with your respective Director and the Permanent Secretary. All staff must not publicly disclose internal MoF information via the Internet that may adversely affect the relations and public image of the Ministry of Finance.

5.5 Access Control

All users wishing to establish a connection with the Ministry of Finance computers via the Internet must authenticate themselves at a firewall before gaining access to MoF internal network.

All users of the MoF computing and networking facilities are expected to get prior approval from the Deputy Director of Information Technology before they establish modems, Internet or other external network connections that could allow non-MoF users to gain access to the MoF system and/or networks and MoF information.

Approval should be obtained from the Deputy Director of Information Technology before users can use new or existing Internet connections to establish new communication channels. These channels include electronic data interchange (EDI) arrangement, electronic malls with on-line shopping, on-line database services.

5.6 Reporting Security Problems

The Information Technology Division must be notified immediately when:

6. Sensitive MoF information is lost, disclosed to unauthorised parties, or suspected of being lost or disclosed to unauthorised parties.
7. Unauthorised use of the Ministry of Finance information systems has taken place or is suspected of taking place.
8. Passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed
9. There is an unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages

Security problems should not be discussed widely but should instead be shared on a 'need-to-know' basis.

Users are urged not to attempt to probe computer security mechanisms on any of the Ministry of Finance sites. If users probe security mechanisms, alarms will be triggered and MoF resources will needlessly be spent tracking the activity.

Unless prior written authority has been obtain from the Deputy Director of IT, files containing hacking tools or other suspicious material may be taken as *prima facie* evidence of unauthorised hacking activity and may expose the user to disciplinary procedures.

9.1 Penalties

Violations of these security policies can lead to withdrawal and/or suspension of system and network privileges and/or disciplinary action