REPUBLIC OF NAMIBIA
Ministry of Information and Communication Technology
Information Technology Authoritative Policy

Information Technology Authoritative Policy

Introduction

The IT Authority Policy identifies the executive responsible for implementing of IT policies and procedures. This is the section responsible for implementation and accountable for implementation. This document serves as authorization from the Permanent Secretary delegating authority to the IT Section for managing the IT environment of the Ministry of Information and Communication Technology, and becomes the basis from which all other IT Policies will be drafted and implemented.

REFERRING DOCUMENTS

The policy is developed to comply with relevant legislation and policies, including the Information and Communications Act, Act 8 of 2009 for the Republic of Namibia, the Copyright and Neighboring Protection Act no.6 of 1994, the Public Service Act no. 13 of 1995, Acceptable Use Policy and the IT Standards and Procedure guide of the Ministry. Users should familiarize them with these Policies, Acts and guides.

PURPOSE

Information Technology (IT) resources are defined as:

- Capital assets (Servers, monitors, computers, laptops, I-pads, printers, mobile phones, network points, network cabinets, network equipment, switches, routers, servers and biometric systems)

- Software (commercially licensed packages or proprietary configurations/packages)

- Intellectual capital (user files, proprietary database information, operations data, manufacturing and production control data, electronic correspondence, voice mail)

This Policy establishes the authority of the Permanent Secretary to develop, implement, assess, and maintain IT Policies, Procedures, and any other IT related Instructions for the Ministry of Information and Communication Technology.

SCOPE

This Policy applies to the entirety of the Ministry of Information and Communication Technology.

OBJECTIVE

The broad goals of this Policy are to:

- Establish the recognized and dully authorized Directorate\Section for managing IT assets within the Ministry of Information and Communication Technology
- Delegate full authority, responsibility, and accountability for the directing of the IT Policy

RESPONSIBILITY AND AUTHORITY

It is the responsibility of the Permanent Secretary to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted.

POLICY

A. IT Section is accountable for, responsible for, and authorized to establish IT Policies, Procedures, and any related working instructions.

B. IT Section is responsible for communicating IT Policies to Ministerial employees.

C. Human Resource Section is responsible for communicating IT Policies to newly appointed employees.

D. All employees are expected to abide by all IT Policies.

E. Approved Policies remain in effect and are replaced only at the issuance of a new or revised Policy.

F. The Permanent Secretary is authorized to set emergency, temporary policies that may take effect immediately.

G. All employees will have electronic and/or paper access to all IT Policies.

REPUBLIC OF NAMIBIA
Ministry of Information and Communication Technology
Information Technology Authoritative Policy

Information Technology Authoritative Policy

Introduction

The IT Authority Policy identifies the executive responsible for implementing of IT policies and procedures. This is the section responsible for implementation and accountable for implementation. This document serves as authorization from the Permanent Secretary delegating authority to the IT Section for managing the IT environment of the Ministry of Information and Communication Technology, and becomes the basis from which all other IT Policies will be drafted and implemented.

REFERRING DOCUMENTS

The policy is developed to comply with relevant legislation and policies, including the Information and Communications Act, Act 8 of 2009 for the Republic of Namibia, the Copyright and Neighboring Protection Act no.6 of 1994, the Public Service Act no. 13 of 1995, Acceptable Use Policy and the IT Standards and Procedure guide of the Ministry. Users should familiarize them with these Policies, Acts and guides.

PURPOSE

Information Technology (IT) resources are defined as:

- Capital assets (Servers, monitors, computers, laptops, I-pads, printers, mobile phones, network points, network cabinets, network equipment, switches, routers, servers and biometric systems)

- Software (commercially licensed packages or proprietary configurations/packages)

- Intellectual capital (user files, proprietary database information, operations data, manufacturing and production control data, electronic correspondence, voice mail)

This Policy establishes the authority of the Permanent Secretary to develop, implement, assess, and maintain IT Policies, Procedures, and any other IT related Instructions for the Ministry of Information and Communication Technology.

SCOPE

This Policy applies to the entirety of the Ministry of Information and Communication Technology.

OBJECTIVE

The broad goals of this Policy are to:

- Establish the recognized and dully authorized Directorate\Section for managing IT assets within the Ministry of Information and Communication Technology
- Delegate full authority, responsibility, and accountability for the directing of the IT Policy

RESPONSIBILITY AND AUTHORITY

It is the responsibility of the Permanent Secretary to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted.

POLICY

A. IT Section is accountable for, responsible for, and authorized to establish IT Policies, Procedures, and any related working instructions.

B. IT Section is responsible for communicating IT Policies to Ministerial employees.

C. Human Resource Section is responsible for communicating IT Policies to newly appointed employees.

D. All employees are expected to abide by all IT Policies.

E. Approved Policies remain in effect and are replaced only at the issuance of a new or revised Policy.

F. The Permanent Secretary is authorized to set emergency, temporary policies that may take effect immediately.

G. All employees will have electronic and/or paper access to all IT Policies.

....

Mbeuta Ndjarakana
Permanent Secretary
Ministry of Information and Communication Technology

COMMUNICATION TECHNOLOGY
OF THE PERMANENT

UNITY LIBERTY JUSTICE

REPUBLIC OF NAMIBIA

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY

IT Standards and Procedures Guide

2014

REPUBLIC OF NAMIBIA

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY
Information Technology Standards and Procedures Guide

Table of Content

1. IT Steering Committee

1.1 The Role of the IT Steering Committee

The Information Technology Steering Committee is to provide overall leadership and direction to the implementation and procurement of information systems, software and hardware in the Ministry.

1.2 The Constitution of the IT Steering Committee

The Chairperson of the Information Technology Steering Committee shall be the Permanent Secretary of the Ministry.

In his/her absence, the chairperson shall be his/her delegate or the person on management who represents the Ministry on the Public Service Committee on IT.

Members of this committee shall be the Chief Systems Administrator, the person who represents the Ministry on the Public Service Committee on IT as well as four senior officers (Management Cadre) of the Ministry appointed by the Permanent Secretary.

1.3 Terms of Reference of the IT Steering Committee

The Information Systems Steering Committee shall:

(a) Set goals and objectives for the development of information systems and technology and draft short and long-term project proposals for the Ministry.
(b) Provide overall direction and leadership for the computerization of the Ministry.
(c) Endorse the acquisition of hardware, software and other IT-services for the Ministry.
(d) Submit Tender proposals and any other computerization plans to OPM-DPSITM for approval. The Department of Public Service Information Technology Management will not process any IT request without the written consent of the IT-steering committee.
(e) Provide direction on procurement of IT-equipment and or enablers for staff-members.

2. Physical Access Control

2.1 Entrance Doors

(a) All entrance doors will be fitted with an access control reader (Biometric and or card readers) and a magnetic door lock to allow access to authorized personnel only.
(b) All doors will be fitted with a hinge on the door to ensure that entrance doors are always closed.
(c) Each staff member fingers will be scanned on to the Access Control System in order to get access to his/her office or floor which they are authorized to.
(d) In the case that a staff members finger cannot be read by the Access Control System reader the IT-Section should be informed immediately as to rescan his/her finger on the System.
(e) Key control of office's and any other doors which is not fitted with a Biometric reader is the responsibility of the Auxiliary Section, all copies of keys in circulation should be sign in and out from the key control register which will be with the Auxiliary Section.

2.2 Server Room

(a) Door to the server room will be kept locked and keys will be with the IT-Section only.
(b) Access to the server room will be restricted to personnel of the IT-Section only.
(c) Other staff or contractors that require access to the server room will notify the IT-Section in advance.
(d) Adequate air-conditioning should be installed to provide a stable operating environment in order to reduce the risk of any system failure due to systems that have crashed.
(e) All contractors or other staff members working in the server room need to be supervised at all times by a member of the IT-Section.
(f) No water, rain water or drainage pipes should run adjacent to the server room to reduce the risk of flooding.
(g) An Uninterruptible Power supply will be installed in the server room and be configured to do a proper shut down of the system in case of a power failure.

2.3 Servers, Workstations (computers), Tablets (ipads) and laptops -- (Access Unit)

(a) All staff members of the Ministry are responsible for securing their computers, tablets and or laptops from unauthorized use, damage and theft.
(b) Whenever a user away from his/her access unit the unit should be protected by either logging off or locking the access unit by pressing simultaneously ALT, CONTROL, and DELETE.
(c) Laptops, tablets or any other portable devices should never be left unattended in an open area or office.

(d) At the end of a working day each user/staff member is required to shut-down his/her unit, unless otherwise advised by the IT-Section.
(e) Users are not allowed to consume food or drinks near or on their computers/workstations.
(f) Under no circumstances are visitors allowed to work on workstations/computers except with the approval of management.
(g) In case of theft or damage to any IT-equipment, the IT-Section and Stock Control unit should be notified immediately in writing and a police case should be opened when a theft has occurred.
(h) Theft and damages to equipment will be dealt with by the Loss Control Committee.

3. Logical Access Control

3.1 User Identification, Authentication and Authorization

(a) Authorization/Access to the Ministry's network and access units will only be granted through individual username and password.
(b) Each user is responsible for actions performed while his\her user-id is in use on the network.
(c) Users will only be given rights to folders and information systems needed to perform their work. User access will be kept to a minimum.
(d) User access and rights will be reviewed as and when the need arise.
(e) Users will not be given rights to change their log-on credentials, nor to change their computer settings
(f) Users will log-on to the Ministry's network by entering in capital letter the first letter of their name followed by small letters their surname (Jdoe), and their password.
(g) Passwords will have an alphanumeric string of at least 8 letters and numbers (eg. Mine6789)
(h) Username and passwords should under no circumstances be shared.
(i) Passwords should be hard to guess and easy to remember.
(j) Passwords will expire every 90 days and the last 3 passwords used cannot be re-used.
(k) The user account will automatically lock after 3 incorrect log-on attempts.
(l) Users will not have rights to delete any of their own folders on the file-server; this is to prevent accidental deletion of folders.
(m) The Personnel section shall notify the IT-section of any employee leaving the Ministry; this is in order for them to disable the account of the user that has resigned.
(n) Network and server administration passwords will be stored in a secure location to prevent unauthorized access to these systems.

3.2 Server and Access Unit Security

(a) All operating systems and applications will be kept up to date.
(b) The IT-Section will ensure that up to date anti-virus scanning software is installed on all Servers and Access units (computers).
(c) Users will not be granted any rights on the anti-virus software except for scanning of their systems or removable drives in use.
(d) Servers and Access units must be scanned at least once a week for viruses or when there is irregularities detected on the network.
(e) All servers should be stored and lock away in the Server room.
(f) Remote Access will on be granted to IT Personnel on the Servers.
(g) Domain Controllers and File-Server system auditing must be enabled for unsuccessful logon attempts
(h) System log should always be backed-up to a safe and secure location.
(i) All Sun Solaris system accounts will be password protected.
(j) Only IT Personnel will be allowed to log-on to the Servers.
(k) Windows encryption will be enabled for password encryption, no clear text passwords will be allowed.
(l) The IT Section will ensure that anti-virus renewals are done in advance to ensure continuity of the anti-virus system software and to prevent the software from becoming unlicensed.
(m) No removable media (external drives, USB's or dongles) will be used on the Ministry's network unless it's scanned via the Ministry's anti-virus software.
(n) No user will be allowed to upload or install any software or shareware on their Access Units.
(o) In the event of a possible virus infection, users must notify the IT Section immediately to contain or delete it to prevent it from spreading on to the network.
(p) Users will be held accountable for any breach of this virus protection procedure.
(q) The IT section personnel shall do regular checks on desktop, laptops and tablets for the presence of any unauthorized software, music and movies and delete them as per the policy of this Ministry.

3.3 Internet and E-mail security measures

(a) E-mail for all authorized users will be configured on the server.
(b) Anti-virus software will be installed on the e-mail server to scan all e-mail for viruses and malware.
(c) A firewall will be installed between the Ministry and Office of the Prime Minister – Department Public Service Information Technology Management to prevent unauthorized internet activities on the Ministry's network.
(d) Users are not allowed to send bulk e-mails, advertising e-mail, spam mail, chain letter e-mails or any other unauthorized e-mails to any employee of the Ministry or use the Ministry's network to send such e-mails.
(e) Internet usage will only be allowed as per Acceptable Use Policy of the Ministry

4. LAN (Local Area Network) and WAN (Wide Area Network) Security

(a) All LAN and WAN equipment such as router, switches, hubs, wireless access points, wireless routers, etc. will be stored and locked in a secure place.
(b) All networks used by the Ministry will be fully documented with diagrams showing the physical and logical layout of the networks.
(c) Users must not store or place any item on top of the network cables.
(d) Access to the system consoles and server disk's will be restricted to IT Personnel only.
(e) The IT Section will keep a full inventory of all network, computer and software equipment in use at the Ministry.
(f) Users will not be allowed to install their own wireless network equipment onto the Ministry's network.
(g) All wireless LAN equipment will make use of the most secure encryption and authentication facilities available.
(h) All connections to the internet will be made via the firewall (proxy server) to prevent access to unauthorized sites and downloads.

INFORMATION AND COMMUNICATION TECHNOLOGY
OFFICE OF THE PERMANENT SECRETARY

....

Mbeuta Ua-Ndjarakana
Permanent Secretary
Ministry of Information and Communication Technology

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Information Technology Security and Procedures Policy

VERSION 1

2014

REPUBLIC OF NAMIBIA

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY
Information Technology Security and Procedures Policy

Table of Content

1. INTRODUCTION

Information security is becoming increasingly important, the Ministry of Information and Communication Technology is becoming more and more dependent on use of computer systems. These dependencies, as well as the introduction of new technologies that brings new risks, underlines the necessity of an information technology policy for the Ministry of Information and Communication Technology.

Information exists in many forms, stored on computers, across networks, printed or written on paper, stored on tapes and compact disks. Therefore, this policy is to ensure that all information and computing assets of the Ministry of Information and Communication Technology are properly safeguarded to achieve a secure environment for both our customers and our staff.

This policy defines the minimum mandatory standards that need to be implemented to protect this Ministry from threats to the security of our information, networks and Information Technology assets\equipment, whether their nature is deliberate or accidental or whether they arise from internal or external sources.

The mandatory standards are grouped into 3 categories to protect all information and IT Assets/equipment:

- Authoritative IT procedures
- Acceptable Use Policy
- Standards and Procedures guide

This policy should be used in conjunction with the Security Rules and Regulations, compiled by the Public Service Committee on IT and the IT Policy for the Public Service of Namibia vol. III

2. POLICY STATEMENT

It is the policy of the Ministry of Information and Communication Technology to ensure:

- The confidentiality and integrity of information.
- The availability of information, data and services to meet the business requirements of the Ministry
- That regulatory and legislative requirement is met.
- That Information Technology usage training is available to all staff.
- That any breach of information security, actual or suspected, is reported and investigated.
- That the IT-Standards and Acceptable use procedures are adhered to.
- That all IT-assets are protected and safeguarded against theft and or vandalism
- This policy will be reviewed annually.

Responsibilities:

- It shall be the responsibility of the IT-Section to ensure that procedures and guidelines are in place to provide adequate protection and confidentiality of all information, data, information technology equipment and software systems to ensure continued availability of information and programs to all authorized users.

- Every staff member has the responsibility to comply with the information technology usage and procedures guidelines as set out by this policy and to take reasonable precautions to protect all Information Technology equipment and information they use in the performance of their duties.

- The responsibility of this policy rest with the Permanent Secretary (Accounting Officer) of the Ministry of Information and Communication Technology.

3. STATUTORY AUTHORITY

The policy is developed to comply with relevant legislation and policies, including the Information and Communications Policy for the Republic of Namibia 2008, the Copyright and Neighboring Protection Act no.6 of 1994, the Public Service Act no. 13 of 1995, the Acceptable Use Policy as specified by the Office of the Prime Minister.

The aim of this IT-security and procedures policy is to ensure that the data is safeguarded, always available and complete.

Note should be taken of the following acts and articles:

- Article 13(1) of the Constitution on the Fundamental Right of Privacy.
- The Communications Act, Act 8 of 2009
- Also take note of the provisions of Section 25 on misconduct as set out in the Public Service Act 1995, where these have direct implication on the misuse of IT resources.
- The Copyright and Neighbouring Rights Protection Act, 1994 (Act no 6 of 1994) and the regulations promulgated there under. Also find application in cases where computer software is used under licensing conditions.

- The Government has the right to access and disclose the contents of electronic files as required for legal, audit or legitimate operational or management purposes of the Public Service.

4. WARNINGS/CORRECTIVE ACTIONS

The Ministry of Information and Communication Technology will review complaints or instances of unacceptable use brought to its attention in accordance with the prescribed procedures as set out in the Public Service Staff Rules. Violators of the IT-policies and procedures of the Ministry of Information and Communication Technology are subject to corrective action and discipline in accordance with the provision of the Public Service Act, 1995 and other relevant legislation.

5. Summary of IT Standards and Usage procedures

5.1 Confidentiality of all data is to be maintained through access controls.

5.2 Passwords must consist of at least 8 alphanumeric characters and must be changed at least every 90 days. The Domain Controllers will not allow you to use any of your last 3 passwords.

5.3 Internet, e-mail and any other external services (USB's, external drives) is to be used in conjunction with the Acceptable Use of IT equipment procedures.

5.4 Only authorized and licensed software may be installed on any desktop computer, laptop or Ipad, and installation may only be done by staff from the IT-Section. In the event of unauthorized software being detected, it will be removed from these devices immediately.

5.5 All removable media from external sources must be scanned to check for viruses before they are used on any computer, laptop or server of the Ministry

5.6 Computer and laptops configurations may only be changed by staff from the IT-Section, and only authorized changes may be done.

5.7 To prevent loss of any information, regular back-ups on the file server, domain controllers and must be done as per the back-ups procedures of the Ministry.

5.8 All computers must be configured with a z-drive in order for staff-members to back-up critical information on to the File-Server.

5.9 No music and movies are allowed to be stored on user computers or on the z-drive of the File Server or any other network drive.

5.10 All servers and network storage devices must be fitted with an Uninterruptable Power Supply to prevent damage to the servers in case of a power outage.

5.11 IT-Equipment such as laptops, Ipad's and software that needs to be procured should be signed off by the IT-Section with an approved submission by the Directorate's Director and the Permanent Secretary.

Approved:

…………………………………………………………

M. Ua-Ndjarakana

Permanent Secretary: Ministry of Information and Communication Technology

INFORMATION AND COMMUNICATION TECHNOLOGY

PERMANENT SECRETARY

REPUBLIC OF NAMIBIA

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY

ACCEPTABLE USE POLICY

2014

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY
Acceptable Use Policy

ADMINISTRATIVE USE

The AUP (Acceptable Use Policy) serves as a fair-use notice to all Ministry of Information and Technology employees; violations of fair-use may result in disciplinary actions as according to the Public Service Staff Rules. The Acceptable Use Policy should be incorporated into your new hire packet for employees. Existing employees should be presented with the AUP. A signature on this document confirming acknowledgement by all employees is preferable. You should retain the executed copy of this policy in the employee's file indefinitely..

REFERRING DOCUMENTS AND MATERIAL

- IT Policy for the Public Service of the Republic of Namibia Vol. III 2003/2004
- Information Technology Security and Procedures Policy of the Ministry of Information and Communication Technology Version 1 of 2013.

PURPOSE

Information Technology (IT) resources are defined as:

- Capital assets (monitors, computers, desk-set phones, laptops, servers, IPAD's, mobile phones, network points, printers, Biometric access points and any other IT-related equipment)

- Software (commercially licensed packages or proprietary configurations)

- Intellectual capital (user files, proprietary database information, operations data, manufacturing and production control data, electronic correspondence, voice mail)

The Ministry encourages the use of its IT resources for legitimate business activities. The Ministry strictly prohibits employees from using technology inappropriately as defined by this policy or from exposing the Ministry to potential liability.

SCOPE

This AUP applies to all employees and consultants working for the Ministry of Information and Communication Technology.

CONSEQUENCES

Misuse or abuse of Ministerial IT resources through willful violation of the AUP will result in disciplinary action leading up to and/or including termination or further legal action.

OBJECTIVE

The broad goals of this policy are:

- Protection of intellectual proprietary owned by the Government of the Republic of Namibia
- Protection of capital assets and the safe guard against misuse
- Protection of data integrity and confidentiality
- Prevention of unlawful conduct
- Minimize the Ministry's exposure to liability
- Prevention of downtime, loss of mission-critical data, or productivity loss

RESPONSIBILITY AND AUTHORITY

It is the responsibility of the Permanent Secretary of the Ministry of Information and Communication Technology to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted.

POLICY

A. **Ministerial employees and consultants are prohibited from**:

1. Using Ministerial technology assets for commercial use, "for-profit" commercial activity, product advertisements, gambling, harassment, terrorism, political or religious lobbying, or any form of discrimination (including but not limited to: race, gender, national origin, age, marital status, sexual orientation, religion, or disability).

2. Sending unsolicited bulk and/or commercial messages over the Internet- E-mails ("spamming").

3. Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including copyrights, trademarks, service marks, trade secrets, software piracy, and patents held by individuals, corporations, or other entities.

4. Engaging in activity that violates privacy, confidentiality, publicity, or other personal rights of others, employees, corporations, or other entities.

5. Using Ministerial IT resources to advertise, transmit, store, post, display, or otherwise make available pornography of any kind or obscene speech or material.

    a. The working definition for pornography that will be used for enforcing this policy shall be: “Verbal or pictorial explicit representations of sexual behavior that . . . have as a distinguishing characteristic the degrading and demeaning portrayal of the role and status of the human figure as a mere sexual object to be exploited and manipulated sexually."

6. Using Ministerial IT resources to distribute defamatory, harassing, abusive, or threatening e-mails.

7. Forging or misrepresenting any form of message headers, whether in whole or in part, to mask the originator of the message, packet, or datagram (“spoofing” or “smurfing”).

8. Accessing illegally or without authorization computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system ("hacking").

9. Any activity that might be seen as a precursor to an attempted system penetration (i.e. port scan, stealth port scan, NetBIOS scan, or any other information gathering activity on the Ministry’s network).

10. Willfully distributing Internet viruses, worms, Trojan horses, pinging, flooding, mail-bombing, or denial of service attacks.

11. Any activities that disrupt the use of or interfere with the ability of others to effectively use the Ministry's network or any connected network, system or service, is also prohibited.

12. Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP, which includes the facilitation of the means to spam, initiation of pinging, flooding, mail-bombing, denial of service attacks, and piracy of software, is strictly prohibited.

13. Engaging in activities that are determined to be illegal, including advertising, transmitting, or otherwise making available pyramid schemes, fraudulently financial activities, and pirating of software. Employees should be cognizant that engaging in any activity that the Ministry determines to be harmful to its operations, reputation, goodwill, or supplier relations violates this AUP.

B. **<u>Ministerial employees and contractors are compelled to:</u>**

1. Abide by all AUP requirements.

2. Abide by all IT Policy requirements.

3. At all times, conduct their online activities as professional representatives of the Ministry, conscious of our reputation and customer's interests.

4. Access only the data and files that the employee owns, is authorized to view, or is made available publicly.

5. Remain conscious of who might have access to their workstation, laptop, PDA, or mobile phone; employees should restrict the use of these materials to Government business only.

6. Lock their computer and/or log off their computer, lock filing cabinets, and secure confidential information when away from their desks or offices.

7. Avoid wasting scarce resources on the Ministry's assets (bandwidth, drive space, printer paper and toner) or monopolizing systems for their own use.

8. Obtain permission from the Permanent Secretary before publicly sharing information about the Ministry, its officers, managers, staff, or other employees, or its customers.

9. Report suspicious activities and breaches in security to the Ministry's management immediately.

10. Respect the Copyright Laws of the Republic of Namibia (concerning illegal copying of software, distribution of copyrighted content, or plagiarism).

C. The Ministry of Information and Communication Technology will take actions consistent with the objectives of this policy to protect its technology investments. Activities include but are not limited to:

1. Immediate removal of illegitimate (unlicensed) software.
2. Immediate removal of pornography and illegitimate movies.
3. Immediate removal of hazardous devices, software, email, or user files which could prove harmful to the Ministry's computing environment.
4. The monitoring of employee activities on the Internet or on the Ministry's Intranet.
5. The limiting of individual access or capabilities.
6. The forensic investigation into the acceptable use of the Ministry's assets.
7. The physical thievery or piracy of hardware, software, copyrighted materials, or operations data is not tolerated under any circumstances.

D. Ministerial employees should presume any degree of privacy whatsoever in the context of providing electronic mail (e-mail) to its employees.

1. The Ministry reserves the right to examine, delete, or alter email content to protect and maintain their systems and to uphold the purpose of this policy.
2. The Ministry discourages the forwarding of externally derived jokes, graphics, screen savers, or programs that are prohibited by this policy.
3. The Ministry's management presumes that employees will take care in crafting their correspondence to reflect professionalism, courtesy, and respect.
4. Only authorized personnel are permitted to investigate the electronic information of employees on Ministerial resources.

E. The Ministry will make every effort to educate its employees on the acceptable use of its information resources as time, ability, and necessity permit.

F. Only software approved and purchased by the Ministry will be installed on Ministerial computers.

INFORMATION AND COMMUNICATION TECHNOLOGY
OFFICE OF THE PERMANENT SECRETARY

....

Mbueta Ua-Ndjarakana
Permanent Secretary
Ministry of Information and Communication Technology