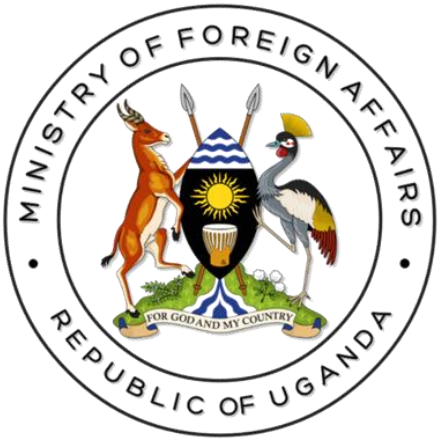

Information and Communication Technology Policy

Table of Contents

Acronyms / Abbreviations

BYOD	Bring Your Own Device
CIA	Confidentiality, Integrity and Availability
ICT	Information Communication and Technology
IT	Information Technology
LAN	Local Area Network
MOFA	Ministry of Foreign Affairs
MOU	Memorandum of Understanding
PMIS	Protocol Management Information System
PS	Permanent Secretary
PPDA	Public Procurement and Disposal
OS	Operating System
NITA U	National Technology Authority of Uganda
USB	Universal Serial Bus

Foreword

In the year 2003, Ministry of Foreign Affairs commissioned the first ever (ICT) policy. From that time to date, there has been a lot of technology changes. The Ministry has heavily invested in technology infrastructure and therefore depends on technology for service delivery. This is geared towards increasing effectiveness and efficiency in all the Ministry's functions. It is deemed necessary to review and develop more relevant guidelines

The development of this policy took into consideration alignment to other existing Ministry functional policies as well as globally recognized ICT practices. The policy will be reviewed periodically to ensure it remains relevant and aligned to the Ministry strategic objectives. Therefore, from time to time it will be necessary to modify, add and amend some sections of this policy and procedures

The Ministry's ICT Policy provides a structure for all the relevant ICT policies to support the achievement of the ICT Vision. Broadly, the policies here spell out best practice, define roles and responsibilities of all user groups as well as provide guidance in the delivery, implementation and usage of ICT.

Users are required to comply with all the guidelines in this policy as well as local and international laws and to refrain from engaging in any activity that would subject MOFA to any liability.

Lastly, I wish to acknowledge the efforts of the ICT Steering Committee and the ICT Division in coordinating the development of this policy.

…….
Amb. Patrick S. Mugoya
Permanent Secretary

1.0. Background

In its pursuit to enhance its mandate of promoting and protecting Uganda's interests abroad, the Ministry of Foreign Affairs recognizes the use of ICT as an enabler to facilitate access to public services by her populace through the use of e-Government. E-Government is about the use of information and communication technologies and the Internet to improve the delivery of services by government to its citizens and the business sector. The ICT Policy will provide guidance on how the use of ICT will facilitate interactions within government(s), between government and the citizens, business and citizens, government to business to simplify and enhance its internal and external communications.

The Ministry of Foreign Affairs has been investing huge resources in ICT infrastructure in order to serve her populace better. Because of the nature of the Ministry structure, being spread globally and therefore serving the whole world, a robust communication system is eminent.

The Ministry recognises the rate at which technology evolves both for opportunities and threats as well. Cybercrime has become a matter of concern to most institutions globally. As communication over the internet is the way to go, information is increasingly becoming a target by the adversaries. Never the less, the Ministry's information must remain confidential but available to the intended beneficiaries without being tampered with.

Therefore the Ministry needs guidelines to protect the ICT infrastructure and the information that is transmitted or stored using this infrastructure.

The users of the ICTs; employees, contractors, venders / suppliers must be guided on how to maximally reap the benefits of the infrastructure.

Despite the heavy investment, the opportunities, the risks and threats involved, the Ministry has been lacking guidelines on how to acquire, protect and use the right equipment. Having a document in place that spells out the guiding principles on how to select, use and protect these important facilities is just timely.

The policy is important to protect the integrity of MOFA's computing facilities and its users against unauthorized and improper use, and to investigate possible use of those facilities in violation of Ministry's rules and policies.

1.1. Situational Analysis

Information Technology has emerged as the single most important enabler for improving efficiency and effectiveness of organizations. “Electronic Governance” is the term that is being used as a synonym to describe an IT driven system of governance that works better, costs less and is capable of serving the citizens’ needs.

Recognizing the enormous potential of IT, major initiatives are being implemented by the Ministry such as a robust website as a centre of communication, the official email system, social media platforms like whats-app, twitter and Face book. The Ministry is also pursuing to implement a Protocol Management Information System (PMIS). The Ministry established its own Local Area Network (LAN) to facilitate these initiatives. These good initiatives can be strengthened and yield results if they are backed by clear guidelines.

However, there are still some challenges in the use of IT by the Ministry to pursue her mandate. These must be checked especially when it comes to implement commercial and economic diplomacy.

Most employees prefer to use personal emails like the yahoos, gmails, hotmails which are unreliable, unsecure and therefore not recognized by government as official channels of communication.

The unlimited access to the ICT facilities puts the Ministry at risk as the adversaries can exploit the weakness that can put the Ministry in disrepute.

Sometimes electricity is not reliable which renders the network unavailable. Due to dependence on the internet, no work is done when the network is off.

Lack of skilled manpower is also another internal challenge. The ICT division at the Ministry Headquarters is highly understaffed with IT professionals.

An ICT policy will give guidance on how to overcome these challenges.

Despite the challenges there are also number of opportunities that can be tapped to make the use of ICT fruitful.

1. A number of legislations pertaining to the IT industry have been put in place. Laws related to Intellectual Property Rights, Data Security, Privacy, Data Protection and cybercrimes have been enacted although some are still in infancy and enforcement is still low.
2. The government has laid the National Backbone Infrastructure (NBI) that connects most of the MDAs and Local Governments.
3. Fibre cables already laid down by the private sector which are strategically laid in the more profitable urban areas. This has reduced the cost of access to the internet.

There are a number of threats that face the ICT sector which include physical, administrative, and technological ones. Access to the ICT infrastructure and technological threats like malwares need to be dealt with.

Therefore this policy will help the Ministry to maximise on the strength, correct the weaknesses that exist, tap into the opportunities and guard against the external threats that the ICT sector faces as shown above.

1.2. General Scope

This policy applies to all the employees of the Ministry of Foreign Affairs headquarters, and the Uganda's Missions abroad. It also applies to software contractors, and vendors / suppliers who provide services to MOFA that bring them into contact with MOFA's ICT infrastructure. This policy covers the following areas:

I. ICT use
II. Technology Hardware and Software Acquisition
III. Management and Use of Software
IV. Bring Your Own Device (BYOD) for official use
V. Security of Information Technology
VI. Business continuity and Disaster Recovery
VII. Information Technology Administration
VIII. Official Email Management and Use
IX. Website Management
X. Management of ICT Service Agreements
XI. Emergency Management of Information Technology
XII. Use of Social Media

2.0. Policy Vision

A ministry where ICT is a central tool used in implementing Uganda's Foreign Policy

2.1. Policy Goal

To enhance institutional efficiency and effectiveness through appropriate regulation and administration on use of ICT products to enhance Uganda's Foreign Policy and protect Uganda's image abroad.

2.2. Policy mission

To deepen utilization of affordable ICT products and services by all members of staff both at the Ministry Headquarters and Missions abroad in promoting and protecting Uganda's interests abroad

3.0. Policy objectives

i. To provide guidelines for the acquisition and use of both ICT hardware and software for the Ministry and Missions abroad
ii. To provide guidelines on the security of information in the Ministry and the Missions abroad
iii. To regulate and control access to the Ministry's ICT infrastructure and resources
iv. To avail guidelines on the administration of ICT infrastructure and other related resources
v. To establish how to deal with emergency issues related to loss of information (in case of a deserter)
vi. To give guidelines on the use of the websites, official mail and social media as communication channels for the Ministry

4.0. Policy Areas and procedures

4.1. ICT Usability

Overview

This chapter entails the guide to the best use of ICT resources in a secure manner. It covers personal use of email, internet, software installation, copyright infringement and prohibited activities. It is meant to define the Ministry's standards for acceptable use of ICT resources.

This applies to employees, contractors, consultants, temporary staff and other workers at the Ministry, including all personnel affiliated with third parties. It also applies to all equipment that is owned by the Ministry.

Procedures

1. Information stored on electronic and computing devices whether owned or leased remains the sole property of the Ministry and must be protected in accordance with the Data Protection Standard.
2. All mobile and computing devices that connect to the Ministry network must comply with the Network Access Policy.
3. System and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
4. All computing devices must be secured with a password-protected screensaver. Users must lock the screen or log out when the device is unattended.
5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

The following activities are strictly prohibited:

1. Under no circumstances is an employee of MOFA authorized to engage in any activity that is illegal under local or international law while utilizing the Ministry's ICT resources.
2. Violations of the rights of any person or the Ministry's protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Ministry.
3. Accessing data, a server or an account for any purpose other than conducting official business is prohibited.
4. Introduction of malicious programs into the network or server (viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Effecting security breaches or disruptions of network communication.
7. Port scanning or security scanning is expressly prohibited unless prior notification to the Ministry is made.
8. Circumventing user authentication or security of any host, network or account.

9. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
10. Providing information about the Ministry's employees to parties outside the Ministry without the authorisation by the PS.
11. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
12. Blogging by employees using Ministry's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Ministry's systems to engage in blogging is acceptable with the authorisation from relevant office

4.2. Technology Hardware and Software Acquisition

Overview

From time to time the Ministry procures ICT equipment in form of hardware as well as software. These include desktops, laptops, communication infrastructure like switches, routers, and servers. The Ministry also procures and installs a range of software; both applications and Operating software (OS). This involves huge amounts of finances and it happens quite often to cope with technological advancement. To ensure compatibility, scalability and value for money, it is imperative to have clear guidelines to regulate this activity.

This chapter therefore provides guidelines for acquisition of both hardware and software for the Ministry to ensure that all the technology for the Ministry is appropriate, ensures value for money and where applicable integrates with other technologies that support E-Government. This is to ensure that there is minimum diversity of hardware and software within the Ministry and Missions Abroad. These guidelines also apply to software obtained as part of hardware bundle or pre-loaded software and software obtained during day to day operations.

Procedures

1. All the procurement of technology will follow the standard procedure as provided for in the Public Procurement and Disposal Act (PPDA)
2. The service provider to be procured must meet the guidelines by the National Technology Authority of Uganda (NITA U)
3. ICT Division will from time to time provide specifications to guide the acquisition of both hardware and software

4. No equipment whether a donation or procured will be put use before verified the ICT division

4.3. Management and Use of Software

Overview

This chapter provides guidelines for the use of software for all employees within the Ministry to ensure that all the software used is appropriate. The use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

1. All computer software copyrights and terms of all software licences will be followed by all employees of the Ministry and Missions abroad.
2. ICT Division will ensure Software licensing terms are followed
3. Head ICT Division will ensure that software audit of all hardware is completed twice a year to ensure that software copyrights and licence agreements are adhered to.
4. All Software to be installed must be appropriately registered with the supplier where this is a requirement.
5. Ministry of Foreign Affairs will be the registered owner of all software installed on her infrastructure.
6. Only software obtained in accordance with these guidelines will be installed on the Ministry and Missions abroad computers.
7. All software installation is to be carried out by ICT specialist.
8. A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

4.3.1. Software Usage

1. Only software purchased in accordance with this policy will be used within the Ministry and mission abroad.
2. Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.
3. All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of Head ICT Division.

4. Unless express approval from Head ICT Division and ICT specialist in missions abroad is obtained, software cannot be loaded on an employee's Personal computer.
5. Where an employee is required to use software on personal computer, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's personal computer, authorisation from Head ICT Division and ICT specialist in missions abroad is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the Ministry and must be recorded on the software register by the ICT Division

4.3.2. Breach of the Guidelines

1. Unauthorised software is prohibited from being used in the Ministry and missions abroad. This includes the use of software privately owned by an employee, contractor and used with the Ministry ICT infrastructure.
2. The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee, who makes, acquires or uses unauthorised copies of software will be referred to the Accounting officer for disciplinary action. The illegal duplication of software or other copyrighted works is not condoned within the Ministry of Foreign Affairs and Missions abroad.
3. Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Head ICT Division immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee will be referred to the Accounting Officer for disciplinary action.

4.4. Bring Your Own Device (BYOD)

Overview

Ministry of Foreign Affairs acknowledges the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have the option of connecting their own mobile devices to the Ministry's and /or Mission's network and equipment.

This chapter therefore provides guidelines for the use of personally owned devices used for official business purposes. These guidelines cover all Ministry employees, contractors, suppliers and

vendors that use or access Ministry of Foreign Affairs' technology equipment and/or services. The devices in question include portable devices; laptops, notebooks, telephones

Procedures

Each employee who utilises personal mobile devices must agree to the following terms:

- To register the device before use including the applications used by the device
- Not to download or transfer the Ministry or personal sensitive information to or from the device. Sensitive information includes all official information not sanctioned for public consumption e.g. MOUs, Treaties, intellectual property.
- To make every reasonable effort to ensure that Ministry's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected.
- To maintain the device with current operating software, current security software and up to date Anti Malware.
- Not to share the device with other individuals to protect the Ministry's data or access through the device
- To abide by Ministry of Foreign Affairs' internet guidelines for appropriate use and access of internet sites.
- To notify Ministry of Foreign Affairs immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to Ministry of Foreign Affairs' equipment.

All employees who have a registered personal mobile device for official business use acknowledge that the Ministry:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data

- Will regularly back-up data held on the device
- Will delete all data held on the device in the event of loss or theft of the device
- Has first right to buy the device where the employee wants to sell the device
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
- Has the right to deregister the device for business use at any time.

4.4.1. **Keeping mobile devices secure**

The following must be observed when handling mobile computing devices:

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

4.4.2. **Indemnity**

- Ministry of Foreign Affairs bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities.
- All staff indemnify the Ministry of Foreign Affairs against any and all damages, costs and expenses suffered by Ministry of Foreign Affairs arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by Ministry of Foreign Affairs.

4.5. Security of Information Technology

Overview

Confidentiality, Integrity and Availability (CIA) of information are very important pillars of any organisation information management. The procedures under this chapter aim at ensuring that these pillars are upheld so that there is no compromise to the Ministry's information and technology infrastructure. Protection against damages and liability created when unauthorized access occurs, and also against threats and physical damages to the infrastructure is emphasized.

This chapter provides guidelines for the protection and use of information technology assets and resources within the Ministry to ensure integrity, confidentiality and availability of data and assets.

This applies to all staff, contractors, consultants, temporary and other workers operating on behalf of the Ministry who have authorization to access Ministry's technology infrastructure

Procedures

Physical Security

- All communication infrastructure (servers, routers, switches and other network assets), must be secured
- Adequate ventilation must be provided
- Appropriate access control measures must always be provided so that only authorized personnel is allowed access to the technology infrastructure
- Security and safety of all portable technology, such as laptop, notepads, iPad will be the responsibility of the employee who has been issued with the device.
- All devices such as laptop, notepads, iPads when kept at the office desk is to be secured by relevant security measure provided by the Ministry.

4.5.1. Information Security

- All Ministry critical data will to be backed up and secured on a monthly basis
- All technology that has internet access must have anti-virus software installed.
- It is the responsibility of Head ICT Division to install all anti-virus software and ensure that this software remains up to date on all technology used by the Ministry.
- All information used within the Ministry is to adhere to the privacy laws and the Ministry's confidentiality requirements.
- Any employee breaching this will face disciplinary actions.

4.5.2. **Network Access**

- All users accessing any of Ministry's network infrastructure must get authorization from the Network administrator
- The access and use of the network resources shall be restricted to official duties only.
- All Wi-fi enabled devices must be secured with password and user authentication
- All computers and devices on the network must be logically and physically secured when leaving them unattended
- All devices must run up to date software applications and properly configured firewall.
- All network resources are the property of the organization and can be subject to monitoring without recourse to the staff and the organization reserve the right to grant or deny access to the network

4.5.3. **Technology Access**

- Every employee will be issued with a unique identification code to access the Ministry technology for example Wi-Fi and will be required to set a password for access to domain services every six months.
- Each password is to be at least 8 characters and alpha-numeric and is not to be shared.
- Head ICT Division is responsible for the issuing of the identification code and initial password for all employees.
- Where an employee forgets the password or is 'locked out' after three attempts, then Head ICT Division is responsible to reissue a new initial password that must be changed when the employee logs in using the new initial password.

The following table provides the authorisation of access:

Technology – Hardware/ Software	**Persons authorised for access**
Desktop computers and laptops	Only Ministry staff.
Internet service (wireless and cabled)	Ministry staff and any other authorised personnel.

Technology – Hardware/ Software	Persons authorised for access
Servers, routers, switches and any other network devices.	Authorised ICT Division staff.
Email- services	Only ministry staff.

It is the responsibility of Head ICT Division to keep all procedures for this policy up to date.

4.6. Business continuity and Disaster Recovery

Overview

The Business continuity and disaster recovery policy presents the Ministry's strategic plan to ensure that critical business functions are available even after a disaster had occurred. This includes identification of critical systems and data, frequency of back up, responsibility of back up administrator, storage of back up, offsite rotation, and restoration procedures. The purpose of this policy is to provide the Ministry's last line of defence in the event of data loss which may occur due to hardware failure, data corruption, or any security incident which may present a threat to critical systems.

Procedures

1. The organization shall classify data in order to identify critical data for backup and recovery purpose as per Records Management Policy.
2. Back up frequency and offsite rotation shall be in accordance with data backup standards and procedure for various systems.
3. Backup storage facilities shall be under lock and key and shall be protected from environmental hazards such as excess heat, water leakage and dust.
4. All critical data must be stored in a media as per current technology and data backup standards.
5. Data retention shall be in accordance with the organization's records management policy.
6. Critical data shall be restored in accordance with the procedures depicted in the disaster recovery plan.
7. Restoration procedures and documentation shall be reviewed annually to reflect developments in the business environment.
8. All back up data shall be tested regularly in accordance with the data backup standards and procedures.

4.7. ICT Governance

Overview

Effective ICT Governance provides a conducive environment for the alignment of all ICT investments in a rationalized manner that is aligned towards enabling the Ministry meet its goals and objectives. This contributes to the attainment of value for money, management of risks and effective ICT utilization.

Procedures

ICT Steering Committee

The Permanent Secretary shall appoint an ICT Steering Committee whose role and duties include:

I. Ensure that ICT strategy is aligned with the strategic objectives of the Ministry
II. Monitoring the quality of the ICT projects
III. Providing advice (and sometimes making decisions) about changes to the ICT projects
IV. Providing support, guidance and oversight function to the ICT Division.

ICT Division

The Division shall be responsible for the day to day running of the ICT activities in the Ministry and these shall include:

I. Coordinate the development of ICT strategy that supports the organization's business objectives and helps build a strong competitive advantage.
II. Support employees to make the most effective use of ICT resources, by providing various forms of user support.
III. Develop and operate a network to support effective communication and collaboration.
IV. Protect the ICT infrastructure and corporate data against attacks from viruses, cybercriminals and other threats.
V. Develop tools to collect, store, manage, secure and distribute data to employees who need access to the latest information to make decisions about strategic, financial and operational issues.
VI. Conduct a technology audit annually to ensure that all information technology policies are being adhered to.

VII. Maintain and manage all service agreements for the Ministry's technology.

4.8. Official Email Management and Use

Overview:

Email presents an integral part of business communication. However, misuse of email can pose many security risks, thus it's important for users to understand the appropriate use of electronic communications.

The main objective of this policy therefore is to give a guide to the acceptable use of official email in conducting the Ministry's communication and reduce risk of email-related security incidents

This policy covers appropriate use of any email sent from the Ministry email address and applies to all staff, contractors, and consultants, temporary and other workers operating on behalf of the Ministry.

Procedures:

1. All staff must be allocated official email accounts for official communication
2. Personal email shall not be used for official communication
3. Email account credentials shall not be shared
4. All official email accounts must be protected with appropriate logon credentials
5. All emails are the property of the organization and can be subject to monitoring without recourse to the staff
6. All staff are strictly forbidden to open attachments received via email messages which are from unknown (if possible) or mistrusted sender(s).
7. Staff may be subject to loss of privileges and/or disciplinary action if found using email contrary to this policy.

4.9. Data and Information Management

Overview

This include data generation, storage, protection and sharing. This part of the policy provides guideline for the management of the data generated and in possession of the Ministry.

- ✓ All data / information generated and / or received at different levels in all forms and in possession of Ministry departments, Divisions and units belongs to MOFA

- ✓ Units responsible for Data / information Processing (Registries, Depository, Resource Centre) shall process the Data / information in their custody for the purpose of easy access
- ✓ Data / information shall be accessed by only authorized personnel
- ✓ Database Administrator shall be responsible for all the electronic information management

4.10. Website Management

Overview

MOFA uses the robust website as the face to the public in terms of information access. Both the Ministry headquarters and Missions abroad use a uniform template to manage and update the content.

This chapter provides guidelines for the hosting, maintenance and update of all relevant technology issues related to the Ministry's websites.

Procedures

There shall be a Website Register kept by the ICT and Communications Division and shall record the following details:

- List of domain names registered to the Ministry
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting
- Security Certificate licence information

4.10.1. Website Content

- All content on the Ministry's websites is to be accurate, appropriate and current. This will be the responsibility of the Department of Public Diplomacy.
- All content on the websites must be approved by Department of Public Diplomacy.
- The content of the websites is to be reviewed frequently for accuracy and relevance by the Department of Public Diplomacy
- Basic branding guidelines provided by Head Public Diplomacy must be followed on websites to ensure a consistent and cohesive image of the Ministry.

- All changes on the website will be done by the ICT and Communications Division considering the security of the website

4.11. Management of ICT Service Agreements

Overview

For the purpose of this policy, ICT Service Agreement means an official commitment that prevails between a service provider and the Ministry. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the Ministry.

This chapter therefore provides guidelines for all ICT service agreements entered into on behalf of the Ministry.

ICT service agreements may include following:

- Provision of general ICT services and equipment
- Provision of network hardware and software
- Repairs and maintenance of ICT equipment
- Provision of business software
- Website design, hosting, maintenance and updates.

Procedures

- All ICT service agreements must be reviewed by the Ministry's legal Department or solicitor general before the agreement is entered into.
- The service agreements shall be approved by the Accounting Officer.
- All ICT service agreements, obligations and renewals will be recorded and a record kept in accordance the records management procures of the Ministry.

4.12. Emergency Management of Information Technology

Overview

For the purpose of this policy, attention is given to the following as ICT emergency issues:

- Internet Failure
- Email Service Failure
- ICT Hardware Failure
- Virus or other security breach
- Website Disruption

This chapter thus provides guidelines for emergency management of all information technology within the Ministry.

Procedures

All Technology failure and disruptions shall be reported to the ICT Division immediately to take necessary action.

It is the responsibility of ICT Division to undertake tests on emergency procedures to ensure that they are appropriate and minimise disruption to Ministry operations.

All actions must be taken immediately to minimise disruption to business operations.

4.13. Use of Social Media

Overview

Social media is a set of online technologies, sites and practices which are used to share opinions, experiences and perspectives. Fundamentally it is about conversation. In the government context, it is a dialogue that happens between Government and its citizens. This means that the level of control assumed from traditional media is replaced with a deeper level of engagement with the public.

This chapter provides guidelines for the proper choice and usage of the Social Media to suit Ministry's specific needs. It establishes basic principles, addresses code of conduct and legal and security issues related to the use of Social Media in the Ministry

Procedures

- The information relayed through Social media to the public must be credible by being accurate, fair, thorough, and transparent.

- What is published shall be consistent with relevant government policies, standards and behaviors
- Only authorized personnel shall use the official Ministry account if it is part of their duties
- Employees/staff of the Ministry shall not publish personal opinions on official social media accounts

5.0. Implementation Strategy

- The policy will be implemented through development and approval of manuals in the areas identified in the policy statement and others that may be relevant in operationalizing this policy
- ICT Division in partnership with the IT Steering Committee shall be responsible for monitoring the implementation and compliance of these policies and where necessary, take appropriate remedial measures
- ICT Division shall ensure the policies' enforcement and Ministry wide dissemination as well as training, awareness and sensitization of this policy
- Violations of the policy areas listed here within shall be addressed by the appropriate Ministry mechanism

6.0. Monitoring and Evaluation

- Realization of the objectives of this policy will require consistent monitoring and evaluation of the outcome indicators.
- MOFA recognises the role of the Ministry of ICT as the overall body that undertakes monitoring and evaluation of the ICT sector in the country. Therefore the Ministry will play a leading role as far as the overall monitoring and evaluation of this policy is concerned.
- In addition, ICT Division of the Ministry with the help of ICT Steering Committee will lead the process of monitoring and evaluation of the ICT programmes and projects at different levels.
- A monitoring and evaluation framework shall be developed to provide guidance.
- The policy shall be subjected to a mid-term review every three (3) years and a long term review every five (5) years in order to cater for the fast rate of technology innovation and advancement.