THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF WATER AND IRRIGATION

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY
(Draft)

January 2016

TABLE OF CONTENTS

Foreword

The Information and Communication Technologies (ICT) Policy for the Ministry of Water and Irrigation aims at guiding the internal deployment of ICT in a cost effective manner to improve service delivery through efficiency and effectiveness. The ICT Policy for the Ministry is aligned with the National ICT Policy (2003), e-Government Strategy (2013), and other circulars and guidelines issued by PO-PSM and e-Government Agency. The National ICT Policy 2003 and e-Government Strategy 2013 has been developed as a higher-level to address the need and role of the application of Information and Communication Technologies (ICT) in improving government services for MDAs.

The ICT Policy for the Ministry of Water and Irrigation is intended to provide a guideline or framework for more coordinated and user driven focus on the use of ICT as part of enabling the water sector development objectives and streamlining the implementation of e-Government Strategy with the Ministry and Sector at large. The ultimate goal shall be systematic ICT deployment within the National and e-Government Standards to facilitate the implementation of Water Sector Development services and Medium Term Strategy for the Ministry of Water 2015 - 2019. The Policy sets ambitious and specific objectives whose achievement will not only support MoWI in delivering better services through ICT, but will also result in cost effective use of the scarce resources for ICT deployment in a sustainable manner.

It is worth noting that based on this policy, the Ministry will develop an ICT Strategy for systematic ICT implementation in reforming and improving the internal working processes, and ultimately making service delivery to the public easier and quicker. Similarly the strategy to be developed based on this policy will also aim in proper utilization of public resources and avoid duplication of efforts in technology and service delivery.

Effective ICT governance requires people to deploy the right technology in the right way for the right reasons, commonly referred to as “people, process and technology”. This policy explores these themes with a view to arriving at the best possible fit to ensure it is achieved.

I now look forward to the delivery of commitments contained in the policy. Through this work, we can achieve a more integrated approach to the development and management of ICT and information systems as we strive to achieve our vision, mission, goals and business strategies within the Water and Irrigation Sectors.

ENG. MBOGO FUTAKAMBA

PERMANENT SECRETARY

Acronyms and Abbreviation

BWBs	Basin Water Boards
CAG	Controller and Auditor General
DDCA	Dar es Salaam Dams Construction Agency
DPs	Development Partners
e-Government Agency (eGA)	Electronic Government Agency
EWURA	Energy and Water Utilities Regulatory Authority
GMS	Government Mailing System
GIS	Geographical Information System
GoT	Government of Tanzania
GovNet	Government Network
IAs	Implementing Agencies
ICT	Information and Communication Technology
ID	Identity
IFRs	Interim Financial Reports
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
IWRMD	Integrated Water Resources Management and Development
LAN	Local Area Network
LGAs	Local Government Authorities
MCST	Ministry of Communication, Science and Technology
MDAs	Ministry's, Departments and Agencies
MDGs	Millennium Development Goals
MIS	Management Information System
MKUKUTA	Mpango wa Kukuza Uchumi na Kupunguza Umaskini Tanzania
MoEVT	Ministry of Education and Vocational Training
MoF	Ministry of Finance
MoH	Ministry of Health
MoU	Memorandum of Understanding
MoWI	Ministry of Water and Irrigation
NB DSS	Nile Basin Decision Support System
NBI	Nile Basin Initiative
IC	Irrigation Commission
OGP	Open Government Partnership
PCs	Personal Computers
PO-PSM	President's Office, Public Service Management
PO-RALG	President Office Regional Administration and Local Government
RCIP	Regional Communication Infrastructure Project
RCIPTZ	Regional Communication Infrastructure Project in Tanzania
SMS	Short Message Service
SQL	Structured Query Language
TCRA	Tanzania Communications Regulatory Authority
TTCL	Tanzania Telecommunications Company Limited
UDSM	University of Dar es Salaam

USSD	Unstructured Supplementary Service Data
UPS	Uninterruptible Power Supply
UWSSAs	Urban Water Supply and Sanitation Authorities
VLANs	Virtual Local Area Networks
VoIP	Voice Over IP
WDMI	Water Development and Management Institute
WPMS	Water Point Mapping System
WRPM	Water Resources Planning and Management
WSDP	Water Sector Development Programme
WSDS	Water Sector Development Services

1. INTRODUCTION

1.1. Background

The Government of the United Republic of Tanzania (GoT), under its National Strategy for Growth and Poverty Reduction (NSGPR/MKUKUTA), has committed to economic growth and poverty reduction, improved quality of life and social well-being, good governance and accountability for its people and for its future generations. The water sector's contribution to the MKUKUTA objectives is outlined in the Water Sector Development Strategy (WSDS) adopted in 2006. The Strategy aims to meet MKUKUTA objectives by: i) scaling up water and sanitation services delivery to achieve Millennium Development Goals (MDGs), ii) establishing a sustainable platform for water resources governance and development, and iii) strengthening sector institutions and enhancing capacity in the sector.

The government's WSDS outlines the first phase of activities (2008-2014) through the Water Sector Development Programme (WSDP I) and will continue supporting the Strategy in the second phase of the Programme (WSDP II), through the five (5) components defined for this new phase: 1) Water Resources Management; 2) Rural Water Supply and Sanitation; 3) Urban Water and Sanitation; 4) Sanitation and Hygiene; and 5) Programme Management and Delivery Support.

Information and Communications Technologies (ICT) have led to sector improvements in areas of knowledge and information management, human resources development and communication. Increasing capacity of using ICT at the Ministry of Water and Irrigation has further been empowered by the growth of a global network of computer networks known as the Internet. It has impacted the way business is conducted, facilitated learning and knowledge sharing and information flows.

The lack of ICT policy and poor harmonization of initiatives within the sector, have led to a random adoption of different systems and standards, unnecessary duplication of effort, and waste of scarce resources, especially through the loss of potential synergies. Therefore, Ministry of Water and Irrigation has decided to put in place a policy framework through which coordinating mechanisms and harmonized strategies might be nurtured. This ICT policy is designed as a guideline governing the use and utilization of Information Resources within the Ministry based on National ICT Policy (2003), e-Government Strategy (2013), and other government guidelines and circulars issued for MDAs such as (i) *''Waraka wa Utumishi Na. 5 wa Mwaka 2009 '', (ii) ''Mwongozo wa Matumizi Bora, Sahihi, na Salama ya Vifaa vya Mifumo ya Teknolojia ya Habari na Mawasiliano (TEHAMA) Serikalini iliyotolewa na Ofisi ya Rais, Menejimenti ya Utumishi wa Umma Julai 2012'', (iii) ''Kanuni za Maadili ya Utendaji katika Utumishi wa Umma kifungu Na 9 juu ya Matumizi sahihi ya taarifa''; (iv)* ''Government Project Review Checklist Version 1.0 of August 2014, (vi) ''Government ICT Projects Review Criteria Version 1.0 of August 2014''.

The policy includes six (6) focus areas, which include ICT Governance, Business continuity, Systems security, Internet usage and confidentiality, Email services, ICT Training, Technology standards, and ICT acquisition.

1.2. ICT Vision and Mission

Vision

The Ministry ICT Policy is aligned to the following vision statement:
‘’To be an effective Ministry providing improved Water and Irrigation Service delivery enabled by ICT by 2020’’.

Mission

The mission(s) of this policy is:

- To transform the Ministry of Water and Irrigation into a modern government entity that utilises state of the art ICT to improve operations and service delivery in an efficient and responsive manner.
- To strengthen oversight, coordination and enhance internal productivity and knowledge sharing across the Sector.

2. STATUS OF ICT IN THE MINISTRY

Ministry of Water and Irrigation has made some progress in deploying ICT. This progress has improved service delivery to the citizens. This progress is being increasingly used to support the implementation of Water Sector Development Programme since 2006/7 for the acquisition, processing and dissemination of information. The use of ICT services tailored to satisfy the diverse information need of the users within the WSDP context.

2.1. Information Management Systems

2.1.1. Water Sector Programme MIS

The Management Information System (MIS) was installed in 2011 as a Web-based system (www.mowimis.go.tz), and it is accessed by all WSDP IAs countrywide for financial & contracts management. Development and implementation of the MIS was a priority measure in the original Results Framework of WSDP, and became really urgent when financial reporting difficulties led to serious disbursement challenges. Its establishment was a priority response measure to the challenges faced by WSDP 1 since 2006/2007. The system has been operationalized and is used by WSDP IAs (MoWI, PMORALG, LGAs, Regional Secretariats, Basin Water Boards, UWSSAs in Regional Centres and Small Towns, and National Projects). The MIS is also accessible to DPs and other interested stakeholders, providing authorized access to some of the reports. The MIS has the following main modules:-(i) Planning and budgeting: definitions of projects, targets and activities. It also is to record activity amounts, source funds committed by DPs, and their disbursements, (ii) Procurement Management: procurement activities, annual work and procurement plans, tenders and contract awards, (iii) Contract Management: management of signed contracts, records on lot references, provider details, contract amounts and phases, addenda, contract payments, (iv) Financial Management: funds disbursed by DPs, flow of programme funds, fund releases to Components, contract and non-contract expenditures by IAs, (vi) Reporting: Reports for all functional areas of the above modules: projects and contracts listings, cash-flow estimates by component, annual budget, procurement plans, payments and balances, awards of contracts, etc.

In order to get assurance of the functionality of the MIS as a tool for financial management in the Water Sector, the reliability and integrity of the data loaded in the system (e.g. IFRs for FY 2007/08 - 2011/12) was reviewed and validated by the Controller and Auditor General (CAG) in its report of 30 August 2012. The IFRs for FY 12/13 & First Quarter for FY 2013/14 confirmed that MoWI was from FY 2012/13 able to produce financial reports including IFRs on a regular and timely basis as per MoU. The MIS facilitates the tracking of fund releases, disbursements, expenditures, and balances. This was quite impossible to do in a timely manner before the use of MIS. Capacity building in the use of MIS has been provided to WSDP

Implementing Agencies and user training and Internet modems has been provided to MoW, PMORALG, MoH, MoEVT, MoF, all LGAs (old & new), Regional Secretariats (old & new), UWSSAs, Water Basin Boards, and National Projects. For the periods 2011 to 2015 about more than 800 staff from WSDP IAs have been trained including Accountants, Water Engineers, Auditors, External Auditors, Planning Officers (LGAs), Technical & Financial Managers (UWSSAs), District Planning Officers, Procurement officers and District Treasurers.

As the use of MIS continues to be potential and expand, some of the features of the system need further enhancement in order to respond to the emerging user requirements. The continual enhancement of the system is inevitable in order to make it operational in a sustainable basis. The enhancements concern immediate and long-term requirements. As Phase-I is coming to a close, the enhancements will be particularly critical for WSDP Phase II. While the Immediate Enhancements of the MIS have been completed, the Up-scaling/Improvement of the MIS will be implemented after information needs assessment and preparation of requirements specifications.

2.1.2. Water Point Mapping System (WPMS)

Water Point Mapping is a planning and monitoring tool used to locate water infrastructure and collecting related information using any available technology, the information that is collected can be used in decision making for different uses. On the other hand, water point mapping system is an integration of hardware, software, methodologies, data, processes and users dedicated to collecting, storing, processing and analyzing water related information and giving feedback for public use.

Original paper-based up-dating using existing institutional framework is soon to be replaced by innovative real-time and mobile technologies. MoWI is piloting mobile technology (SMS), assisted by several institutions (SEMA project by UDSM, Twente University, eGA). Government has reserved a block of services codes for government mobile services for its citizens. MoWI obtained TCRA Certificate of Numbering Resource Assignment for Unstructured Supplementary Service Data (USSD Short code. The use of USSD code will be tested through SEMA project.

2.1.3. Decision Support System (DSS)

The Nile Basin Initiative (NBI), under the support of then Water Resources Planning and Management (WRPM) has developed the Decision Support System for the Nile Basin (NB DSS). The basic purpose of the Nile Basin DSS is to provide a trans-boundary framework for sharing knowledge, understanding river system behaviour, designing and evaluating alternative development scenarios, investment projects, and management strategies; and to support informed, scientifically based rational decision making. As such its primary objective is to create a shared knowledge base, analytical capacity, and supporting stakeholder interaction, for cooperative planning and management decision making for the Nile River Basin. MoWI plan on the use NB DSS is to look on possibilities that information gathered during the execution of the IWRMD projects shall be linked to the NB DSS such that they can be opened and processed further in the NB DSS. The DSS and its central river basin model system directly support an open and participatory multi-criteria decision making process,

considering simultaneously hydrological, socio-economic criteria and environmental criteria and objectives. The Nile Basin DSS works top of the Postgress SQL as its database system where all the data and information is stored.

2.1.4. Water Utilities Information System (MajIs)

Water Utilities Information System (MajIS) is one of the tools used by EWURA to monitor monthly performance of WSSAs, whereby data and information are entered at the respective UWSSA's headquarters and received by EWURA and the Ministry of Water on monthly basis. Apart from the improved efficiency and effectiveness of data collection and reporting, the data stored in the MajIs shall serve to (i) improve accessibility of data and information for monitoring, planning and decision making as well as for dissemination of information to all stakeholders, (ii) support effective management audits with the objective of analysing, evaluating, reviewing and appraising the performance of all commercially operated water utilities. Accessing the system is by authenticated users only but the generated reports are published online by EWURA.

2.1.5. Other Systems

Other systems used by MoWI from various initiatives to improve efficiencies and service delivery include the following:-

i. EPICOR & AMP for the financial management and budgeting of Government financial resources. The Ministry of Finance owns these systems.
ii. Human Capital Management Information System (LAWSON) used by MoWI for processing of human resource data and information. The system is owned by PO-PSM.
iii. Urban Water Authorities (UWSSAs) are also implementing their tailor made systems to support their business processes, including Accounting and Billing systems, and GIS systems for the management of their distribution network and other assets.

2.2. ICT Infrastructure and Services

ICT Infrastructure offers a range of technologies to assist MoWI in running efficiently. These services are essential to the everyday mechanics of MoWI and integral to effective service delivery. These include hardware, software, and networking and they are used to support an overall ICT environment.

2.2.1. Hardware and Software

MoWI has several ICT equipment including computers, printers, scanners, UPS, photocopiers, TVs, network switches, cameras, IP Phones, faxes etc. ICT equipments are procured through government rendering processes. Currently, there are no approved standards guiding the acquisition of ICT equipment for government entities as a result there exists various hardware and software with different specifications.

The use of licensed software has been expensive for the Ministry as most of the software are exported, and also the use of open source software is still a challenge due to lack of expertise. In terms of hardware maintenance the Ministry has been using internal manpower for service but major repairs are sometimes outsourced. Tailor made software or applications are developed using external consultancies through government tendering processes.

2.2.2. Government Mailing System (GMS)

MoWI has deployed government mailing system for official communications in order to avoid the use of disposable mail e.g. gmail, yahoo, etc for official communications. The use of public emails like yahoo for official communication has been identified as one of the sources of security risks for official issues. The effective use of the GMS at MoWI started on January 2015 and currently 81% i.e 407 out of 500 subscribed users are now using Government Mailing System (GMS) for official communications at the Ministry of Water, Basin Water Boards and Water Labs. These include individual, special and group emails. The use of the official GMS has improved timely internal and external communication and information sharing as a result the reduction of operating expenses for the printings of documents.

2.2.3. Internet availability

MoWI is connected to TTCL (ISP) through fiber at 20Mbps, and two connections have been configured, one is RCIP and the other one is Government Network (GovNet). Joining RCIP for Internet services enabled the Ministry to reduce the cost of Internet services by 60% for the same bandwidth of 20Mbps. Benefits achieved through Internet services include efficiency in internal and external communication, sharing of information and documents within the Ministry, Agencies, Development Partners and other WSDP IAs, as a result reduced operating costs that could be encountered by sharing of hardcopies through printing, etc.

2.2.4. Local Area Network

The internal Local Area Network has been improved and all MoWI buildings are connected by Optic Fiber Cables. Improvement of LAN using Optic Fibre facilitated MoWI to qualify to be connected to Government Network (GovNet) coordinated by eGA. The configuration of VLANs completed and enhances internal communications and file sharing through Intranet services or Active Directory Services.

2.2.5. Government Network (GovNet):

Government Network (GovNet) is implemented by e-Government Agency through RCIPTZ with the aim to connect all MDAs, RSs and LGAs throughout the country into single secure, cost effective, scalable, robust, flexible and shared Infrastructure for Information Processing, Storage and Exchange. This is done by eGA through harmonizing and utilizing existing and planned National ICT Infrastructure and Initiatives such as National Data Centres, etc. This will avoid current individual efforts whereby each Government Entity had its own initiatives for acquisition and

operation of ICT Infrastructure, which seem to be costly, duplication of resources, lack of standardization, and difficulties in data exchange.

Already Directorate of Policy and Planning is connecting to GovNet for testing purposes before rollout to all departments and units. Joining Government Network (GovNet) will enhance the use of IT systems deployed in the water sector because all MDAs and Agencies will be connected. Other benefits will include getting free Unified Communications, Lower Cost for Government International Bandwidth (40%- 90% Reduction), 24/7 Service Support, and Cost Saving and Improved Productivity.

Through Government Network, the Ministry has started to use Government Bulk SMS for the purposes of enhancing internal and external communications. Another effort is the use of Voice of Internet Protocol (VoIP) where by the installation of 100 IP – Phones provided by eGA completed. Training of employees on these services started on 22nd December 2015 in phases.

2.2.6. Hosting of MoWI systems

In order to avoid the hosting challenges for the strategic systems and to avoid duplication of efforts in data centres for MDAs, the then MCST has been implementing National Data Center and 25 % will be for Government use. Also, Mini Data Centers as Disaster Recovery for 25% of National Data Center are constructed. The government data centre will enable a shared, secure and robust ICT infrastructure that will provide a computing and hosting platform from which government entities including MoW can deliver better and cost effective public services. The National Data Centre will also provide the following benefits to the Government and Ministry of Water and Irrigation in particular:- (i) Increased Control for ICT resources; (ii) Reduced Scope for Security Risk; (iii) Disaster Recovery and Compliance Cost; (iv) Saving and Improved Operation; (v) Efficiencies, and 24/7 Service Support. Already, WPMS server has been moved to eGA colocation data center. Other remaining MoWI systems will be moved or hosted by e-Government Agency.

2.3. Training

Currently the Ministry is supporting ICT training to employees through on the job training and further knowledge enhancement using educational institutions within the country or with limited number getting ICT training abroad. Other learning techniques used by employees at the Ministry is through seminars, workshops and tailor made training focusing on use of the existing information systems, hardware and software. This kind of training is conducted to WSDP implementing agencies. In general, there is a shortage of well-qualified professionals of ICT in the sector. There is also no established ICT professional profile within the sector. Access to online learning for ICT is still a problem due to infrastructure challenges. Furthermore, regular opportunities for ICT training for all staff are limited due to lack of resources.

2.4. Government Open Data System

The Open Government Partnership (OGP) is a global initiative that aims at promoting transparency, empower citizens, fight corruption and encourage use of new

technologies to improve governance. The United Republic of Tanzania joined OGP in September 2011 and the first action plan for the government as well as water sector in particular completed in April 2012.

OGP implementation in Tanzania is on Phase II that started from FY 2014/15 to 2015/16 whereby the key objective for the Water Sector is to implement Open Data as a Government commitment to Open Data Initiative. Open Data involves making available to the public some important information about progress made by different sectors of the government on implementing their set objectives through the use of the Open Data Portal, which is administered by e-Government Agency (eGA). By making Water Sector data publicly available, a wide range of actors can be brought into the policy process and debate, bringing valuable new ideas and new thinking to policy making and stronger public participation in monitoring and citizen feedback hence bringing more success in the Water Sector. Based on Government Circular on open data (Takwimu Huria) issued on January 2015, already ten (10) data sets for the Water sector has been uploaded on the government open data portal (www.opendata.go.tz).

3. POLICY OBJECTIVES, CHALLENGES AND POLICY STATEMENTS

3.1. General Objectives

The general objective of this policy is to provide a framework and guidance for the systematic governance, coordination, execution, acquisition, disposal, monitoring and evaluation of the ICT infrastructure and services related to the Ministry of Water and Irrigation.

3.2. Policy Focus Areas

Focus areas of this ICT policy are summarized as;

i. Provide a comprehensive ICT framework towards achieving sustainable ICT usage and management to meet Ministry objectives.
ii. To build the knowledge capacity of employees for maximum utilization of ICT facilities and services in order to attain the Ministry's strategic objectives.
iii. To provide the operational ICT guidance in terms of regulations, working instructions and restrictions to ensure adequate security of the information resources (data, software, systems, hardware and devices) based on e-Government standards and guidelines.
iv. To provide the comprehensive procedures and plans for the assurance of business continuity.
v. To provide guidance on systematic software or systems development based on best practice and e-Government standards and procedures.

3.3. ICT Governance

3.3.1. Issues

The Ministry of Water and Irrigation has placed greater reliance in ICT; it is increasingly becoming reliant on the use of ICT and electronic systems for most of its functions. It is therefore imperative to put in place a focused ownership and visionary ICT management capabilities in order to bring reliable ICT environment. ICT governance provides information and knowledge base in assessing business direction, control, strategy, policy, planning, and resource allocation for supporting informed decisions. Without proper ICT governance in the Ministry, all initiatives and efforts cannot be implemented in a sustainable basis due to duplication of efforts and scattered/disjointed ICT projects that cannot support sector strategies and objectives.

3.3.2. Policy Objectives

(i.) To improve ICT management in order to meet sector objectives.
(ii.) Ensure maximum utilization of ICT facilities and services.
(iii.) Improve ICT governance structure for a coordinates initiatives and resources.

3.3.3. Policy Challenges

(i.) Effective mechanisms for policy coordination.
(ii.) Awareness among leadership and employees for getting political will and policy ownership.
(iii.) Prioritizing budgets for ICT projects.
(iv.) Conducive environment for sustainable ICT deployment.
(v.) Addressing MoWI's stakeholder's needs.
(vi.) Integration with other government initiatives.

3.3.4. Policy Statements

(i.) MoWI will establish ICT Steering Committee responsible for approving ICT innovations, budgets and projects.
(ii.) MoWI will deploy ICT systems as an integral part of its strategic plan and facilitate all departments and units to use ICT for improved quality service delivery.
(iii.) MoWI shall build the knowledge capacity of employees for maximum utilization of ICT facilities in order to attain the Ministry's business objectives.
(iv.) MoWI will promote necessary relations and enabling environment to facilitate the cooperation with other Agencies and ICT or e-Government stakeholders in sharing experiences on utilization and exploitation of ICT and e-Government.
(v.) MoWI will allocate annual budget for maintaining and deploying ICT systems.
(vi.) MoWI shall adopt standards issued by e-Government Agency for acquisition, maintenance and utilization of ICT facilities and services.
(vii.) MoWI shall ensure that all existing systems and proposed systems for data collection, manipulation and storage are streamlined and assessed for its relevancy through ICT Audit based on e-Government guidelines and standards.
(viii.) MoWI will promote the ICT Unit for effective and strategic coordination of the ICT and e-Government policies, strategies and standards within the Ministry and its agencies.

3.4. ICT Standards

3.4.1. Issues

ICT Standards are the written definitions, limits, or rules approved and monitored for compliance in the implementation of ICT projects by MoWI as a minimum acceptable benchmark. Lack of standards results into duplications of the ICT projects as well as procuring ICT hardware and software that do not meet business objectives and costly. ICT standards are a prerequisite for sustainable ICT services such as hardware, data collection, data processing, data storage, database engine, data dissemination, data access, maintenance, repair, and procurement/acquisition/ installation /disposal of software, computer hardware and other general computing devices.

3.4.2. Policy Objective

(i.) Ensure that Ministry adheres to e-Government standards and guidelines for software, hardware and the general computing environment.
(ii.) To streamline or institutionalize e-Government standards for deploying sector systems and hardware specifications.
(iii.) Provide a standardized framework for the procurement, installation, processing, storage, dissemination, access, maintenance and repair.

3.4.3. Policy Challenges

(i.) Awareness creation to management and staff.
(ii.) Technical expertise in the development of standards.
(iii.) Involvement of the ICT staff in the procurement process.
(iv.) Institutionalization of standards and political will and support.

3.4.4. Policy Statements

(i.) MoWI shall obtain ICT and e-Government standards from e-Government Agency and other responsible institutions.
(ii.) MoWI shall ensure that ICT policies and standards are available to staff and being adhered to.
(iii.) MoWI shall ensure that all software installed in the Ministry are licensed in order to conform to copyright rules unless otherwise based on e-Government guidelines.
(iv.) MoWI shall ensure that all software and hardware purchases are within specified e-Government standards.
(v.) MoWI shall ensure that specifications for acquisition of hardware and software are provided or approved by ICT Unit/department.

3.5. Business Continuity

3.5.1. Issues

Management is not only expected to keep the information resources secure, it is also expected to keep MoWI functioning after a disaster or security breach. The activity of keeping the information resources[1] secure is information security management, and the preparations for operating after a disaster, is called business continuity management. The absence of business continuity plan may results in several risks including the risk in the use of information technology resources and loss of data once some threats happened.

3.5.2. Policy Objectives

[1] Information resources refers to computers, network infrastructure, software or systems, and data

(i.) Provide comprehensive ICT procedures and plans for the assurance of business continuity.
(ii.) Establish mechanisms for the implementation of e-Government standards and guidelines on sustainable deployment of the information systems.

3.5.3. Policy Challenges

(i.) Preparation of business continuity plan.
(ii.) Resources for the implementation of policy.
(iii.) Fostering of efficient, inter-operable, reliable and sustainable ICT infrastructure commensurate with MoWI needs and compliant with e-Government standards.

3.5.4. Policy Statements

(i.) MoWI shall acquire and use appropriate computer systems, software and other technologies in the business operation.
(ii.) MoWI shall ensure that all hardware components are made available as timely as required by users.
(iii.) MoWI shall ensure that strategic information are optimally processed and disseminated with minimal disruption.
(iv.) MoWI shall make sure that processes are restored in the event of losing part or all of the computing facilities.
(v.) MoWI shall develop Business Continuity/Disaster recovery plans for all ICT applications to ensure critical data recovery.
(vi.) MoWI shall ensure that all its strategic systems are hosted by e-Government Agency.
(vii.) MoWI shall provide awareness to all employees on Business continuity for the Organization.

3.6. Systems Security

3.6.1. Issue

Storage of MoWI's data on computers or using ICT and transfer across the network eases use in the provision of improved services. Commensurable with that expansion is the need for the appropriate security measures. Security is not distinct from the functionality. The system Security Policy recognizes that not all communities within MoWI are the same and that various departments and units within MoWI use data differently. MoWI has to keep its information resources secure so as to protect its information assets, from IT – related risk. When implementing security controls, the key issues of security versus availability and security versus rights must be addressed.

Systems security policy deals with ensuring systems are available to the organization at all times. The policy deals with equipment, systems environments, information, software and technology security. It defines management, physical and logical security of ICT systems, backup and restores procedures; and enforcement of the same.

3.6.2. Policy Objectives

(i.) Provide guidance in terms of regulations, working instructions and restrictions to ensure adequate security systems and protection of ICT facilities (computer hardware, software and devices) and information against accidental or deliberate damage, destruction, theft or misuse.
(ii.) Protect the data and information resources from misuse but ensure its availability to authorized users who can have confidence in its accuracy and integrity.

3.6.3. Policy Challenges

(i.) Preparation of systems security policy.
(ii.) Human resource for the implementation of systems security policy.
(iii.) Implementation of government standards and guidelines.
(iv.) Staff awareness and political support for policy enforcement.

3.6.4. Policy Statements

(i.) MoWI shall acquire appropriate ICT Systems for managing security issues.
(ii.) MoWI shall create awareness to staff and other users on usage of ICT systems and security requirements for the same.
(iii.) MoWI shall strongly secure information systems, sources, processing, dissemination and resources.
(iv.) MoWI shall ensure that access to computer hardware; information and data files, application software and system software are restricted to authorized users only. Users shall be granted special keys for access.
(v.) MoWI shall provide adequately protected computer systems, software, equipment and devices against natural hazards, theft and damage.
(vi.) MoWI will ensure that licensed antiviruses are installed to all computers based on client-server technology and updated regularly.

3.7. Internet and Email usage

3.7.1. Issue

With the use of Internet and Emails, it is possible to transmit/receive information containing images, graphics, sounds and videos. Internet and email supports linking MoWI with stakeholders and community at large worldwide while taking into consideration security and confidentiality issue.

3.7.2. Policy Objectives

(i.) Provide approaches that ensure optimum and effective utilization of Internet and emails, efficient connectivity, and sound confidentiality.

(ii.) Provide access to a broad range of information resources through optimum usage of Ministry's Internet services and ensuring cyber crime protection and security of facilities.
(iii.) Promote the use of Government or MoWI domains (Government Mailing System) for official communication.

3.7.3. Policy Challenges

(i.) Build an adequate ICT infrastructure within MoWI.
(ii.) Address connectivity and ISP issue.
(iii.) Promote convergence of voice, data, computing, and vide.
(iv.) Internet bandwidth to support MoWI usage.
(v.) Enforcement of Internet and email policy due to resistance for change.

3.7.4. Policy Statements

(i.) MoWI shall prepare and enforce Internet and Emails usage policy based on government standards, circulars and guidelines issued by relevant authority.
(ii.) MoWI shall not use Internet and Emails to transmit confidential, sensitive or proprietary business information without adequate protection.
(iii.) MoWI shall ensure that users are forbidden to use the Internet and emails in a way that violates the privacy rights.
(iv.) MoWI shall ensure that downloading and installation of any program is restricted and shall only be done under the consent of ICT staff.
(v.) MoWI shall ensure that unsecured and malicious Websites are screened/ filtered.
(vi.) MoWI shall ensure that Government Mailing System (GMS) is used for official communications and avoid using other domains (Emails) for official communications such as yahoo, Gmail, etc.
(vii.) MoWI will provide awareness to employees on the proper use of Internet and GMS.
(viii.) MoWI shall ensure that it is connected to Government Network (GovNet) as a single secure, cost effective, scalable, robust, flexible and shared Infrastructure for Information Processing, Storage and Exchange.

3.8. ICT Training (Capacity Building)

3.8.1. Issues

Human capital is the pre-requisite for the effective implementation and use of ICT. MoWI is not the only Government Institution with insufficient numbers of skilled and experienced experts in ICT and in other professionals that rely on ICT. It is therefore necessary to view MoWI's human capital development as a pre-requisite during implementation of ICT services. Human capital development shall consider both technical staff supporting the ICT and all users at the Ministry so as to avoid digital divide. Lack of ICT knowledge and skills lead to less capacity and hence underutilization of information resources which may expose the Ministry to inadequate

information processing and poor communication. The Ministry will strengthen ICT capacity for all users to ensure maximum utilization of ICT resources and facilities.

3.8.2. Policy Objectives

(i.) To increase the quality of ICT skilled human resource base in the Ministry.
(ii.) To provide support for ICT training for Management and all staff with relevant knowledge and skills.
(iii.) Encourage in-house training for staff and knowledge sharing with other MDAs.

3.8.3. Policy Challenges

(i.) Retaining the number of dedicated and qualified ICT professionals.
(ii.) Developing appropriate attitudes, knowledge and skills for ICT initiatives at the Ministry.
(iii.) Resources for supporting ICT training program.

3.8.4. Policy Statements

(i.) MoWI aims to build ICT capacities by training all ICT users to equip them with relevant knowledge and skills, and hence ensure maximum utilization of ICT resources and facilities.
(ii.) MoWI shall conduct ICT training need assessment to determine and plan training requirements.
(iii.) MoWI shall develop and implement ICT training programs based on the result of the ICT training needs assessment.
(iv.) MoWI shall ensure that ICT awareness training to newly employed staff is part of the orientation programme.

3.9. Software or Systems Management

3.9.1. Issues

Managing software or system" and "managing software or system development" is a complex issue, which is surrounded by a lot of challenges. Software project management failures in many organizations has shown that the following are the most common causes:- Insufficient end-user involvement; Poor communication among stakeholders, developers, users and project managers; Unrealistic or unarticulated project goals; Inaccurate estimates of needed resources; Badly defined or incomplete system requirements and specifications; Poor reporting of the project's status; Poorly managed risks; Use of immature technology; Inability to handle the project's complexity; Sloppy development practices; Stakeholder politics (e.g. absence of executive support, or politics between the developers and end-users); and Commercial pressures.

3.9.2. Policy Objectives

(i.) To ensure proper software management based on best practice and e-Government standards and guidelines.

(ii.) To ensure that new software projects are implemented based on e-Government standards, guidelines and checklists.

(iii.) To ensure that requirements specifications become a prerequisite before development or acquisition of new system.

(iv.) To avoid donor dependent software projects to avoid wastage of resources once donor support stops.

3.9.3. Policy Challenges

(i.) Implementation of e-Government standards and guidelines.

(ii.) Top management support to avoid duplications.

(iii.) Controlling donor funded ICT projects and interests.

(iv.) Controlling consultants and/or suppliers.

(v.) Software and system integrations.

(vi.) Controlling rapid change of technologies.

3.9.4. Policy Statements

(i.) MoWI shall institutionalize software or system management practices based on e-Government standards and guidelines.

(ii.) MoWI shall ensure that requirements specifications become a prerequisite before acquisition or development of new software or system.

(iii.) MoWI shall avoid software projects that are donor dependent.

(iv.) MoWI shall ensure that procurement and contract management practices are properly adhered to in any software or system project.

(v.) MoWI shall ensure that enough budget are set aside for the acquisition or design of new software/system covering development costs and operational costs to avoid throw away systems.

4. POLICY IMPLEMENTATION AND MONITORING FRAMEWORK

4.1. Institutional Framework

Because of the multifaceted nature of ICT, the existence of a cohesive and well functioning institutional framework is essential for the attainment of all the objectives of the Ministry's policy. The aim is to ensure that the various departments, units and agencies within the Ministry of Water and Irrigation effectively play their respective roles with a view to promoting effective use of ICT resources and services.

Ministry of Water and Irrigation will provide a leadership and coordination in the Water Sector and in the implementation of the policy objectives based on the National and e-Government strategy, standards and guidelines issued time to time. There will be a need of a strong commitment of the top leadership of the Ministry and at all levels. In order to effectively coordinate and harmonize efforts and activities undertaken by many institutions within the Ministry and sector at large, there is a need to put a mechanism in place which will ensure that policy is updated from time to time and that implementation strategies and plans are drawn and carried out in the most efficient and effective manner based on priority and resource availability in case of new projects needed. The final goal should be the deployment of ICT services in the Water and Irrigation Sectors in a sustainable manner.

Role of the Ministry of Water and Irrigation (Departments and Units)

(a) Deployment, implementation and coordination of the policy.
(b) Monitor the implementation of the policy.
(c) Regular updating of the policy based on business requirements, technological changes and government guidelines and circulars issued time to time.

Role of the President's Office, Public Service Management (e-Government Agency)

(a) Provide regulation, standards, circulars and guidelines for the ICT and e-Government implementation.
(b) Provision of an enabling environment for policy deployment in MDAs.
(c) Provision of technical support for policy implementation.

Role of MoWI Agencies (UWSSAs, BWB's, DDCA, EWURA, WDMI, IC)

MoWI agencies will play a big role in the translation of the policy for effective implementation based on the specific environment of the agency. This will include customization of the policy to meet specific agency and provide high-level support for the policy institutionalization and implementation.

Roles of Development Partners

Development partners will play a complementary role towards realization of the development of the goals and objectives of this policy for the optimal use of ICT in the Water and Irrigation sectors. Within the policy framework, the Ministry of Water and Irrigation through government will foster linkages with various development

partners to provide financial, material, technical assistance as well as build capacity for sustainability.

Role of the Civil Society

The role of the Civil Society will be to make relevant contributions in regard to ICT access, services, data management and e-Governance in order to effectively manage and provide water resources and supply services.

Role of users

Users will be expected to participate in ensuring that quality of services is maintained and continue review of the policy in accordance with technological trends.

4.2. Monitoring and Evaluation Framework

Monitoring framework has been developed as a tool for systematic and routine collection of information in order to support MoWI in policy implementation monitoring. The information collected will facilitate the following with regards to this ICT Policy:-

(i.) To learn from experiences to improve policy in the future.
(ii.) To have internal and external accountability of the resources used and the results obtained.
(iii.) To take informed decisions on the future of the policy.
(iv.) To promote empowerment of beneficiaries of the policy.

Basically, the overall policy monitoring process will allow results, processes and experiences to be documented and used as a basis to steer decision-making and learning processes. This will enable checking progress against expected policy results. Policy monitoring framework has been documented in **Annex 1.**

Annex 1: Policy Monitoring and Evaluation Framework

Area 1: ICT Governance and Control

Policy - 1	**User adherence to ICT Policy and Standard**
Principle	All employees are required to adhere to the policies, standards, and guidelines issued by MoWI and Government.
Objective	To ensure that employees are aware of the appropriate behaviour required when carrying out their roles and responsibilities with regards to ICT.
Risks	Lack of adherence to policies, standards and guidelines may expose MoWI to information risks.
Standards	i. All employees must have access to the available policies, standards, and operational guidelines. ii. Updated policies and standards must be available and communicated to all employees in the Ministry.

Policy - 2	**Deviation and Misuse of ICT Policy**
Principle	Unauthorized deviation and misuse of ICT Policy should be penalized accordingly based on Government regulations.
Objective	To ensure employees are aware of their responsibilities and operational requirements to avoid deviation of Policy.
Risk	Lack of formal procedures for the management of ICT policy could affect the integrity of the ICT environment.
Standards	i. All users of ICT resources have a responsibility to protect the security and integrity of information, equipment and comply with ICT Standards and guidelines issued by e-Government Agency and MoWI in particular. Individuals will be held accountable for their use of information resources. ii. Non-compliance or violation of the ICT policy shall be treated as a major offence punishable according to the provisions in the Public Service regulations. The punishment could includes the following: Suspension, Warning, Demotion; Termination or Dismissal from employment iii. Deviation of the ICT Policies and Standards will require written approval by the Permanent Secretary.

Policy - 3	**Training for ICT users**
Principle	Training for all ICT users at MoWI should be strengthened to ensure maximum utilization of ICT facilities and services.
Objective	To ensure that all ICT users have relevant skills to the utilization of ICT facilities and services available.
Risks	Lack of knowledge may lead to underutilization of existing ICT facilities, services as a result wastage of resources.
Standards	i. ICT Training need assessment must be conducted to all employees. ii. ICT Training programs must be developed based on the training needs assessment. iii. Training must be conducted during the introduction of any new software, hardware or technology as a whole. iv. Allocation of resources (employees, budget, time) for ICT training is important based on resource availability.

Policy - 4	**Personnel Practices**
Principle	All MoWI staff must comply with ICT Policies and Standards.
Objective	To ensure that all MoWI employees are aware of their requirements and their obligations to the utilization of information resources.
Risk	Employees could potentially (unintentionally) breach regulations if policies are not clearly defined, disseminated and understood.
Standards	i. Employees should conduct themselves in a responsible and efficient manner in the course of their duties with regards to ICT usage. ii. All users of information resources have responsibility to protect the integrity of information and equipment. iii. Non-compliance or violation of this security policy shall be treated as a major offence punishable according to the provisions in the Public Service regulations. iv. The ICT Policy shall be disseminated to new employees once reporting or during orientation. v. All employees should be informed on the recovery of expenses caused by the employee in case of breaching the ICT Policies and Standards.

Policy - 5	**Logical Access Control**
Principle	Access to software and information management systems will only be granted to only authorized personnel to perform their day-to-day functions.
Objective	Access to data files, application software and system software should be restricted to authorized users only.
Standards	i. Access control tools should be installed and maintained to agreed standards. ii. Users must only be granted access to the information, data and software that they require to perform their day-to-day functions. iii. User access rights must be established and maintained by the authorized personnel or designated on receipt of an approved request only. iv. All system resources including information, data and software must be protected from unauthorized or accidental access. v. Inappropriate use (such as attempted access or unauthorized execution) of sensitive system utilities must be reported for investigation by the Systems Administrator and followed up with the individual user responsible. vi. Access rights not required for an individual's normal duties should be revoked. vii. Individual access rights should be reviewed when changes to a user's normal duties are required, for example, as a result of a transfer, promotion/demotion.

Policy - 6	**User Access**
Principle	Personnel granted access to Information Management Systems is only entitled to access information and data with the approval of the User Department.
Objective	To ensure that only authorized users gain access to Information Management Systems, and consequently: (i.) Protect the confidentiality of sensitive information and data. (ii.) Protect the integrity of information and data from unauthorized manipulation, fraud and / or damage. (iii.) Protect the availability of this information and data for authorized day-to-day operations.

Risk	Unauthorized disclosure or amendments to information or data stored on Information Management Systems may result in sensitive information or data being disclosed or the integrity of the information or data being compromised.
Standards	i. Access control software, or equivalent features within system software if available, should be used to control access to the information and data commensurate with its classification. ii. Each person requiring access to Information Systems must be individually defined, with each user individually recognizable to the system. No person may use another person's user Id to gain access to computer resources. iii. Users must be defined only once to all environments. iv. Users of the system should not be defined as a Unit or department (i.e., avoid generic accounts). v. Users must be granted access based on the principle of applying the least privilege to achieve the desired function.
Policy - 7	**User ID and Password**
Principle	Every employee assigned a user Id and password is solely responsible for the confidentiality of that password and that an assignee consequences resulting from misuse of the password either by an assignee or by anyone else, is the responsibility of the assignee.
Objective	To ensure adequate password management procedures are maintained throughout the Ministry.
Risk	Lack of strong password management practices could affect the integrity of the computing environment.

Standards	i. Password is to be known only to the individual concerned. ii. Passwords are not to be written down or disclosed to any one under any circumstances. iii. If the user authentication technique is based upon any means which may be duplicated by another user (e.g., passwords): (a) The user must be required to change their authentication code after a predetermined period of time. iv. Users must not be allowed to reuse the authentication code within a set period. v. Passwords should not be obvious, must be kept confidential and not written down and not disclosed by any one by any circumstances. vi. All system users must terminate their active sessions when finished, unless the sessions can be secured by an appropriate lock mechanism. vii. All terminals should be set to time out of 5 minutes or less when left inactive.

Policy - 8	**Segregation of Duties**
Principle	Adequate segregation of duties must exist for all Information Management System functions and between personnel granted access to information and data.
Objective	Adequate segregation of duties must exist to ensure all duties are not assigned to one individual.
Risk	Lack of segregation of duties could result in unauthorized amendment or disclosure of information.
Standards	i. The resource owner or designate must be responsible for ensuring that all duties are not assigned to one individual. ii. Systems administrators should not be involved in the day-to-day input of data.
Policy - 9	**User Responsibilities / Accountability**
Principle	i. The protection of all information system resources (i.e., hardware, applications and system software, data and documentation) is a fundamental responsibility for all employees at the Ministry. ii. Information System resources are required to be used for official or government purposes only.

	iii. Users will be held accountable for all activities performed using their personal user identification.
Objective	To ensure that Information Management System resources are maintained and utilized in the most efficient way possible and they are used for legitimate MoWI and government purposes only.
Risks	i. There may be an inefficient use of Information Management System resources. ii. Unauthorized access and use of Information System resources may result if resources are not adequately managed/ safeguarded.
Standards	The use of information system resources must be for the authorized only for Ministry and government purposes only.

Polic - 10	**Resource Ownership**
Principle	Owners will be assigned to all system resources with responsibility for its integrity.
Objective	To ensure responsibility is assigned for all system resources.
Risk	An increased risk of unauthorized disclosure or amendments being made to the information system.

Standards	i. Information must have clear and undisputed owner. ii. The Resource information Owner is responsible for: (a) Defining the business requirements for which the information, software and / or hardware is needed. (b) Establishing the value, classification, and criticality of Information Technology components. (c) Establishing, maintaining, documenting, and verifying controls with the standards at a cost commensurate with the risk. iii. Resource Owner will have final responsibility over the resource integrity and security control. The Resource Owner will always be responsible for ensuring that all aspects of the Policy / Standards have been met, whether they have been delegated or not. iv. The Resource Designate is responsible for: (a) Developing, operating, supporting and / or monitoring Information Technology resources on behalf of the owner. (b) Collecting, handling, storing and / or disposing of the information on behalf of the owner. However the resource owner should be consulted in the case of disposing. (c) Advising the Resource Owner of any development that could affect the integrity / security control of the resource. v. The Resource Owner or designate must be responsible for the integrity and availability of the resource. vi. The Resource Owner or designate must be responsible for approving access to the resource.
Policy -11	**Usage of Stationary**
Principle	MoWI stationary (e.g., letterhead forms, logo, etc) must be used for valid official reasons only.
Objective	To ensure that MoWI is not associated with non-core related activities.
Risk	Association with non-business related activities might influence the way the public views the MoWI's information management
Standards	Employees are not allowed to use official or government information resources for unrelated businesses.

Policy -12	**Resource Classification**
Principle	All resources will be classified in accordance with their importance and sensitivity to the Ministry.

Objective	Resources should be protected in accordance with their sensitivity to the Ministry, which require specific security controls due to sensitivity or importance should be identified.
Risk	Sensitive resource information may be disclosed to unauthorized personnel, and / or legislative requirements may be breached resulting in embarrassment to the Ministry.
Standards	(i.) All information and data should be classified based on Government Policies and Circulars as follows:- (a) **Restricted** - Information and data of the highest value to MoWI, disclosure which could seriously prejudice the Government, or individual personnel. (b) **Private and Confidential** - Information and data of high value to MoWI, disclosure of which could prejudice MoW, or individual personnel; (c) **Confidential** - Information and data of value to MoWI, disclosure of which could prejudice personnel; and (d) **Unclassified** - Not requiring any additional restriction apart from standard government information security requirements. (ii.) Government Circular No. 2 of 2015 issued on 02 January 2015 on Open Data System (Takwimu Huria) can be adhered to.

Policy -13	**Management Responsibility**
Principle	Management is responsible for implementing and managing security controls within their area of jurisdictions.
Objective	To ensure management is aware of their responsibilities regarding the development of appropriate security practices and the implementation of MoWI ICT Policy and Standards.
Risks	Without sufficient management commitment the policies and standards may not be institutionalized, effectively implemented and enforced.
Standards	MoWI management must support the implementation of ICT Policy**.**
Policy - 14	**ICT Coordination**
Principle	All ICT components that may affect/impact Information Security will need to be reviewed by the ICT Committee or MoWI Management Team prior to implementation/modification.

Objective	To ensure that the MoWI's ICT environment's integrity is not affected by error or malicious action.
Risk	Unauthorized changes could potentially weaken MoWI's computing environments.
Standards	The ICT Committee should be formed comprising of representative from different Departments to coordinate the approval and implementation of ICT projects and security measures of new business critical systems.

Policy -15	**Modification to Software and Systems**
Principle	Only authorized amendments will be made to software or systems based on requirements specifications and required procedures.
Objective	Only authorized modifications will be made to software or systems in accordance with approved change control procedures. This will ensure that changes will not affect the integrity of Information Systems or data.
Risk	Inappropriate changes to software or systems may be made which result in a loss of data integrity, systems availability and / or data confidentiality.
Standards	(i.) Head of ICT Unit/Department must ensure that requirements specifications are prepared before any modification to software or system at MoWI. (ii.) Head of ICT Unit/Department with support of implementation team, prior to the amended version going into production must review documentation of all software or system releases and supplied fixes to software. The review must ensure that the documentation accurately reflects the modified status of the system. (iii.) New releases of software or system, supplied fixes and in-house changes to software or system must be fully tested in a test or development environment prior to implementation in the production-processing environment. (iv.) New releases of software must be documented in accordance with e-Government documentation standards. (v.) All previous versions of the software or system must be available to enable recovery should the new release or modification fail. (vi.) Written procedures must exist to enable the recovery of the previous version of the software or system should the new release or modification fail. (vii.) All changes / modification to software must be performed via the change control mechanism.

Policy - 16	**ICT Environment Change Control**
Principle	Changes to ICT environments (hardware & software) must be controlled.
Objective	In order to minimize the corruption of information systems, all system updates must be properly controlled and managed.
Risk	Inadequate control of changes to ICT environments is a common cause of system or security failure.
Standards	(i.) An assessment of the proposed system update must be performed to assess its potential impact to the MoWI computing environment (ii.) All proposed system updates must be authorized by the application owner or designate and the implementation committee. (iii.) The Head of ICT Unit is responsible for keeping all documentation related to the changes. (iv.) A backup of the module must be made prior being updated. The backup copy must be stored in an archive library. A minimum of 2 backup versions must be maintained.
Policy - 17	**Hardware Purchasing**
Principle	All hardware should be purchased from authorized dealers or suppliers and should contain relevant specifications as issued by the ICT Unit based on Government standards and specifications given from time to time.
Objective	To ensure only hardware that complies with government wide standards are purchased for MoWI.
Risks	(i.) Incompatible hardware may result in the inefficient use of resources or require additional expenditure to enable interface to existing environment. (ii.) Purchasing hardware with different standards that do not comply with MoWI or government standards may lead to difficulties in usage and additional costs in training and maintenance.
Standards	(i.) All hardware should be purchased from authorized or licensed dealers or suppliers. (ii.) All requests for hardware should be sent to the Head of ICT Unit who will provide the specifications based on required usage before submission to Procurement Unit for acquisition and installation. (iii.) Procured ICT equipment must be verified by inspection committee comprising with ICT experts with regards to specific equipment or hardware type. (iv.) Payments for the procured ICT equipment or hardware must be done after getting duly signed inspection report unless otherwise specified in the contractual terms.

Policy -18	**Description on Safe Use of the ICT Hardware and Software**
Principle	Descriptions will be provided to all users during the issuing of equipment or software, or as near as possible to the date it is received.
Objective	To ensure all users are more productive by having been adequately trained in: (a) The use of hardware and software; (b) The functionality of their equipment or software; and (c) Good practices to adopt.
Risk	The following may result if users are not aware of the functionality of their equipment or hardware and appropriate procedures to adopt: (a) Physical damage to equipment through misuse; (b) Loss of data or production of inaccurate information due to the incorrect use of hardware or software; (c) Breach of systems security through the misuse of hardware or software.
Standards	i. Appropriate training (in-house) should be scheduled and conducted for all users, which enable them to understand and use their hardware and software efficiently and effectively. ii. Training should be part of terms of conditions in the procurement and supply of new hardware and software.
Policy -19	**Management of Printed Output**
Principle	All printed output containing sensitive information must be controlled and only available to authorized personnel.
Objective	Hardcopy printouts should be available to authorized users only and must not be amended prior to distribution.
Risk	Hardcopy printouts containing sensitive information or data may be available to unauthorized personnel. Output could be amended or misused prior to being received by the authorized recipient.
Standards	i. Access to printing devices must be restricted to staff or the output owner only. ii. Access to hardcopy output containing sensitive government information and data must be restricted and distributed to authorized recipients only. iii. Printing should be controlled in order to avoid misuse of printing papers.

	iv. MoWI should discourage or minimise the use of stand-alone printers and promote the use of shared printers in order to minimise printing costs (toners, papers, and maintenance costs of the printers).
Policy - 20	**Monitoring, Evaluation and Review of the ICT policy**
Principle	The ICT environment (s) should be reviewed annually and be performed by an ICT Committee to provide assurance that the MoWI practices properly reflect the ICT Policy and Standards and that they are coordinated.
Objective	To provide independent review of the ICT environment at MoWI base on ICT Policy, standards and guidelines.
Risk	The lack of independent will potentially prevent senior management from relying on the integrity of the review.
Standards	i. An independent person must perform ICT Policy reviews (audit). ii. If Internal Audit is not available or is unable to perform the ICT Policy review/information security review, the management should consider a third party organization (External Auditors).

Area 2: ICT Standards

Policy -1	**Use of Unauthorised Software**
Principle	MoWI under no circumstances will tolerate to make use of unauthorized software by personnel within the Ministry.
Objective	Only software that has been purchased and authorized for use will be used within the Ministry
Risk	An illegally copy of unauthorized software may result in the introduction of viruses or similar malicious software, which compromise the integrity of MoWI computing environment. In addition, unauthorized software may result in fines or other associated penalties to the individual user at MoWI.
Standards	i. No unlicensed software or pirated software is to be used on MoWI computer environment. ii. Designated software custodians must ensure that software, once installed on a system, is not copied other than for backup purposes. iii. System administrators should ensure that installation of software in computers is controlled and be performed by authorized staff only.

Policy -2	**Approved Software**
Principle	All software purchased will be selected from an approved or authorized vendor and will comply with the e-Government standards.
Objective	To ensure that only software, which complies with e-Government standards, is purchased and used.
Risk	Incompatible software may result in the inefficient use of resources or require additional expenditure to enable it interface to existing environment.
Standard	(i.) All software should be purchased through reputable and authorized dealer or vendor only. (ii.) Only software, which complies with e-Government standards, should be included on MoWI approved software list. (iii.) All requests for software must be sent to the Head of ICT Unit for an approval before submission to Procurement Unit for acquisition and installation. (iv.) As appropriate, corporate licenses must be obtained for MoWI as possible.

Area 3: Business continuity

Policy -1	**Backup and Recovery Procedures**
Principle	MoWI will ensure that LAN Server based software, information and data files are backed up regularly to enable the system to be recovered when required and without loss of integrity.
Objective	In the event of a system malfunction or disaster to enable software, information, and data to be recovered when required and without loss of integrity.
Risk	Loss of information, data or software, which cannot be replaced without considerable effort and cost to the Ministry.
Standards	(i.) ICT Unit to ensure that a backup of all software, information and data is undertaken on a basis commensurate with the frequency with which that software, information or data changes. (ii.) All backups must be stored in a secure location and on removable media (i.e. external Hard Disk, CDs and tapes), remote from the operations environment to which they belong (i.e. this means storing the backup media at a different geographical location, such as another building). (iii.) A cycle of off-site backup storage must be implemented for all critical or strategic systems. Off-site is defined as a

	facility or building physically separate to the one in which the hardware is located and to which access would be possible even if the facility is unavailable. (iv.) Off-site backups should be promptly in the event of an emergency.
Policy- 2	**Backup Procedures**
Principle	All systems software, application software, information, data and associated documentation will be backed-up to enable the system to be recovered when required and without loss of integrity.
Objective	Enable processing to be restored in the event of losing part or all of the computing facilities.
Risk	Information, data and software could be lost or corrupted if it is not backed-up correctly and on a timely basis.
Standard	(i.) Critical backups of vital records data and systems documentation should be stored securely at a remote location away from the main computer site. (ii.) During transportation to and from remote storage locations, back-up media should be protected with defined levels of physical security. Logs recording the contents of back-up media held in remote storage locations must be maintained and secured. (iii.) All Information Systems should be backed up on a regular basis. The system backup cycles should be performed before and after major changes to the operating system (system software), such as software upgrade; (iv.) Ensure application software is backed up after each change (e.g. following a new release of the application or following maintenance to the production software); and (v.) Ensure that all information and data is backed up commensurate with the frequency with which it is changed. All information and data should be backed up daily if it is changed that day. (vi.) A cycle of backups should be used with at least one copy in each cycle stored off-site. Off-site is defined as a facility or building physically separate to the one in which the computer system is located and to which access would be possible even if the main facility is unavailable. Copies of all operations, and application system software and user documentation should be stored off-site. (vii.) Backups held on-site should be stored in a secure area and only be accessible by authorized personnel. The off-site storage facilities should be restricted to authorized personnel only; and provide adequate protection against fire, flood, dust and physical disasters.

	(viii.) Responsibility for the definition of appropriate backup cycles should rest with the Resource Owner or their designate. (ix.) Backup copies of critical / sensitive information must be provided with the same level of physical and logical controls as provided to the originals. (x.) Recovery Plans should be documented for all systems.
Policy -3	**Disaster recovery Plans**
Principle	Appropriate Disaster recovery Planning for all systems will be developed and tested by the ICT Unit to ensure recovery when required.
Objective	Disaster recovery Plans should be developed for all applications to ensure critical applications can be restored on a timely basis.
Risk	The loss of critical applications may result in a significant loss of business to the Ministry.
Standards	The ICT Unit will be responsible for the development and maintenance of Systems Disaster recovery Plans.
Policy 4	**Hardware Maintenance**
Principle	All hardware components (Workstations, Servers, UPS, printers, etc) will be covered by appropriate maintenance schedule, which will provide for the timely replacements or repair of equipment in the event of a failure.
Objective	To ensure all hardware components are available as required by users and that the optimum amount of MoWI business can be processed with minimal disruption.
Risk	Hardware components malfunctioning can result in equipment not being available for an extended period of time. In addition, hardware failures may result in critical information and data being corrupted.
Standards	(i.) Appropriate maintenance schedule should be established and regularly reviewed for all hardware. The management should approve these schedules. (ii.) Appropriate maintenance schedule should include: • Formal Contracts; and

	• Maintenance Schedule arrangements. (iii.) Maintenance schedule should provide adequate coverage to meet Service Level Agreements and the requirements of users. These requirements should include the provision of replacement hardware if required.

Policy -5	**Computer Virus Control**
Principle	i. Only authorized information, data and software from officially recognized sources, or passed through MoWI screening procedures, may be used. ii. All PC's, Workstations, must be adequately protected against viruses.
Objective	To ensure that information, data and software are protected against viruses.
Risk	Viruses may affect the stability of the computer system and may contribute to the damage or loss of valuable business information.
Standards	(i.) Antivirus software must be installed on all workstations to ensure all data and software received from other machines is scanned, preferably on an isolated Workstation, prior to use. (ii.) Personal computers (e.g., notebooks, laptops) should be scanned daily for viruses, as part of the re-boot process. Bypass of the inbuilt scanning process is strictly prohibited. (iii.) All information or files electronically down-loaded from the Internet into workstation must be scanned before being used. (iv.) All e-mail and their attachments should be scanned before entering into government e-mail system. (v.) If a virus attack is suspected the following must be observed: (a) Suspect removable disks must be isolated; (b) Suspect personal computer must not be used; and (c) ICT Unit must be informed immediately. (vi.) No disks containing unauthorized data and programs, from outside can be used on MoWI PC's (i.e., games disks, code written on home PC's, etc). (vii.) The infected Workstation should be isolated (i.e. physically disconnected from all networks) to prevent future

	usage until the virus has been removed. (viii.) The ICT Unit should be responsible for the removal of the virus and investigation of its origin. (ix.) System Administrators (Hardware and Software) should run antivirus software on all their network file servers on a regular basis (preferably daily). (x.) Any electronic information being brought into MoWI ICT environments (i.e. removable disks) must be scanned before use.

Policy -6	**Documented Operating Procedures**
Principle	Clearly documented operating / management procedures should be prepared for all operational computerized systems.
Objective	To ensure complete and appropriate operational documentation is available for the operational management of the hardware and software.
Risk	The lack of clear operational documentation could potentially prevent an inexperienced user from properly performing his / her functions.
Standards	i. Documented procedures shall specify the correct instructions for the detailed execution of each job, including as appropriate the following: (a) The correct handling of data files. (b) End Of Day and Beginning Of Day system status, (c) Instruction for handling of errors or other exception conditions. (d) Support contacts in the event of unexpected operational or technical difficulties. (e) System restart and recovery procedures for use in the event of system failures. ii. Documented procedures must also be prepared for system housekeeping functions associated with computer and network management. iii. Documented procedures shall be treated as formal documents, and changes shall only be made after approval by authorized management.

Area 4: Systems security

Policy- 1	**Security Awareness Programs**
Principle	All employees will be informed of the importance of ICT Systems Security through computer security awareness programs.
Objective	To increase the awareness of Information Systems security within MoWI and create an environment with sound computer security practices.
Risks	A lack of Information & Communication and Technology Security awareness may result in sub-standard procedures and practices being in place, thereby compromising computer security across MoWI.
Standards	(i.) All MoWI employees should undergo appropriate computer security awareness programs so that they understand the potential threats to Information Systems and their specific systems security responsibilities. (ii.) All employees are responsible to keep themselves informed of new security policies or of changes to the existing policies / standards. (iii.) The Head of ICT Unit is responsible for producing Security Awareness programs on a regular basis.
Policy - 2	**Storage of Software**
Principle	All media (e.g. diskettes, Flash Disks, CDs, magnetic tape) used to store software / data must be securely stored at all times when not in use.
Objective	Software should be securely stored so as to enable full recovery of the application environment in the event of a hardware malfunction or disaster.
Risk	Software stored in an insecure manner may result in software not being fully recoverable as a result of a hardware / software malfunction or disaster situation.
Standards	i. Software CDs are to be stored in lockable storage areas. ii. The ICT Unit is responsible for all software management and safekeeping.
Policy -3	**Software Disposal**
Principle	All software will be disposed in a manner, which complies with Government standards. The disposal and associated actions will be required to be authorized by the Management after consultation with responsible authority and details recorded in the Software Register.
Objective	To ensure all software is disposed appropriately and unauthorized users must not obtain access to information and data.

Risk	Software not being disposed of appropriately may lead to confidential information and data being obtained by unauthorized personnel and licensing agreements being breached.
Standards	(i.) Software must be erased so it is in a non-readable format prior to disposal. (ii.) All disposals of software must be authorized by the Permanent Secretary or designated Officer and details recorded in the Software Register.
Policy 4	**Hardware Disposal**
Principle	All hardware equipment (e.g., Workstations, Servers, UPS, printers, etc) equipment will be disposed of in a manner, which complies with Government circulars and Standards. The disposal and associated actions are to be properly authorized and details recorded in the hardware register.
Objective	All hardware equipment will be disposed of in an appropriate manner that will ensure that confidential information and unauthorized personnel do not obtain data.
Risk	Hardware equipment being disposed inappropriately may lead to confidential information and data being obtained by unauthorized person.
Standards	i. Obsolete or damaged equipment should be disposed off in one of the following ways: • Traded in on replacement equipment; • Transferred to another Department/Unit; • Sold for written down value or trade in value, which ever is the higher or Scrapped. ii. All erasable software, information and data should be removed from storage devices prior to disposition. iii. Disposals should be approved based on Government guidelines, circulars and standards. iv. Obsolete diskettes and tapes containing confidential or restricted information must be forwarded to the ICT Unit for disposal.
Policy -5	**Portable Electronic Device Protection**
Principle	A custodian of computer equipment (e.g., notebook, Modems, etc) has the responsibility to protect the security and integrity

	of information and computer equipment.
Objective	To ensure that portable components located outside the Ministry's controlled environment are properly safeguarded and accounted for.
Risk	Portable equipment may be accessed by unauthorized users or stolen.
Standards	i. A User / custodian of computer equipment shall protect valuable removable equipment, including portable computers from the threat of theft or loss. ii. All Information Technology components must contain an identification number. iii. ICT Unit must maintain a permanent record of ICT equipment identification number (e.g. model description, etc).
Policy -6	**Physical Security Controls**
Principle	All critical Information systems areas (e.g., computer server room) must be properly controlled to prevent unauthorized access, damage, and interference with Information Services.
Objective	Physical security of computerized facilities is necessary for two main reasons. Firstly, to prevent unauthorized use of computer equipment, and Secondly, to ensure that computer equipment is adequately protected against natural hazards, theft and damage.
Risk	Inadequate physical controls over critical areas could potentially affect the integrity of MoWI information environments.
	i. Physical access to computer server room must be restricted to authorize employees that need access to perform their normal duties. Any access to third parties for the purpose of maintenance or support should be supervised. ii. Hazardous and combustion materials should be stored at a safe distance from the site. Computer supplies such as stationary should not be stored in the computer room until required. iii. Fall back equipment and back-up media should be stored at a safe distance to avoid damage from a disaster at the main site.
Policy -7	**Control of Environmental Conditions**
Principle	MoWI will establish appropriate management practices to ensure environmental conditions (fire, water, humidity dust and temperature) are adequately controlled.
Objective	To establish and maintain adequate environmental conditions over Information & Communication Technology hardware components.

Risk	Inappropriate fire, water, dust and water management practices could potentially have a severe impact on physical environments.
Standards	i. Computer equipment must be housed in an environment equipped with: Air conditioners; Regular maintenance of the Air conditioners; and Locked doors and windows to prevent dust. ii. Computer equipment must not be located in areas susceptible to water seepage. iii. The computer environment should be maintained to meet the machines operating tolerance restrictions as recommended by the manufactures of the equipment. Air conditioning equipment should be provided and it should not be possible for the failure of a single component to disable the entire system.
Policy - 8	**Physical Security of the Workstations**
Principle	All workstations located within MoWI premises will be protected against unauthorized physical access.
Objective	To ensure that all access to a workstation and its components are restricted to authorized staffs.
Risk	Unauthorized users could potentially gain access to information in the Workstation hard disk.
Standards	i. Workstations will be assigned to individuals. Accesses to these workstations are restricted to personnel or authorized consultants or technicians. ii. No sensitive information should be stored in the unprotected shared resources. iii. The relocation of computer equipment (e.g., printer, terminal, non portable peripherals) will only be performed by ICT Unit.
Policy - 9	**Identification of Hardware and its custodian**
Principle	(i.) All ICT hardware (e.g., workstations, printers, etc) will be physically identified as being owned by MoWI and the designated custodian will be responsible for the management of the equipment/hardware. (ii.) All ICT hardware will be used only for official business, wherever physically located.
Objective	All hardware should be readily identifiable as MoWI equipment and used only for related business.
Risk	The portability of ICT hardware components increases the possibility that they may be lost or stolen. Sensitive information and data may be revealed to unauthorized personnel.
Standards	i. All Workstations and Portable computers (laptops) and associated peripherals should be marked with a unique MoWI identification code.

	ii. ICT Unit and Procurement Management Unit should maintain a register of Desktop and Laptop computers as per Government Circular. This register may include among others the following details: • Component model; • Component make; • Purchase Date; • Designated Custodian; • Transfer Date; • Serial No. etc. iii. The hardware details should be entered into the hardware register prior to being issued. iv. The designated custodian should acknowledge the receipt of hardware in writing at the time of installation. v. The designated custodian of the ICT component will only remove equipment from MoWI premises with the written approval of the Procurement Management Unit in consultation with ICT Unit. The purpose is to keep register updated. vi. All hardware should be returned to the premises as soon as possible after the designated custodian completes the required work or upon termination of their employment or contract. vii. All employees are not allowed to use Laptop computers for personal business and must ensure that designated laptop is kept within MoWI premises/offices for security purposes in case of loss.
Policy -10	**Physical Network Connection**
Principle	The physical connection of any equipment to the network or LAN will only be allowed after approval by the ICT Unit or designate. All requirements for an external connection will be reviewed on an annual basis.
Objective	To ensure that all physical connections to the network, whether local or external, are authorized. In addition, the requirement for external connections should be reviewed on a regular basis to ensure that only connections that can be justified with a legitimate business case are installed.
Risk	A lack of appropriate physical access controls across networks may result in unauthorized access to MoWI information and data. This could lead to unauthorized amendments or disclosure of government information and data.
Standards	i. The ICT Unit must ensure that all network and server equipment including LAN-Servers are secured from unauthorized access. These should be placed in locked rooms.

	ii. Those components of the network located in the premises controlled by MoWI must be protected with physical access controls. iii. The ICT Unit is responsible for ensuring that records and diagrams describing all computer hardware attached to the network backbone are maintained up to date. iv. Physical access must only be granted with the approval of the Head of ICT Unit or designate. v. The identity of the user accessing the system must be positively validated prior to the connection being completed. The validation should be performed by the user being required to enter a unique user identifier (User-Id) and password every time they access the system.
Policy -11	**Media Security**
Principle	All media (e.g., CDs removable hard disks, diskettes, magnetic tape) used to store information or data should be securely stored at all times when not in use.
Objective	Information and data should be stored securely so as to enable a full recovery of an application in the event of a software / hardware malfunction or disaster.
Risk	Information and data stored in an insecure manner may result in an application not being fully recoverable as a result of a software / hardware malfunction or disaster situation or potentially accessible to unauthorized people.
Standards	i. ICT Unit must ensure that a backup media of all information and data is undertaken on a basis of the system / application business requirements. ii. All backup media should be stored in a secure location, remote from the system to which they belong (i.e. this means storing the backup media at a different geographical location, such as another building). iii. Backup media of production environments must have a cycle of off-site backup storage implemented. Off-site is defined as a facility or building physically separate to the one in which the hardware is located and to which access would be possible even if the main facility is unavailable. iv. Physical access to the tape library must be strictly controlled. v. Media containing sensitive information must be disposed of securely and safely.

Area 5: Internet and Email Usage

Policy -1	**Usage of Internet**
Objective	To ensure that the Internet service is used appropriately and for valid business use.
Risk	The Internet service could be used in a way that could affect the reputation of the Ministry.
Standards	(i.) It is forbidden for staff to use the Internet in a way that violates the privacy rights. (ii.) Internet access should never be used for personal gain or other activities that might be interpreted as illegal or unethical. (iii.) Data or other information downloaded from any Internet site must be scanned for viruses. (iv.) The Internet must not be used to transmit confidential, sensitive or proprietary business information without adequate protection. (v.) Viewing and downloading pornography is strictly prohibited.
Policy -2	**Transmission of Sensitive Information via E-Mail**
Principle	Government Mailing System (GMS) shall be used by all employees for official communications.
Objective	To ensure that sensitive information does not fall into the hands of unauthorized individuals.
Risk	Sensitive information, which is accessed by unauthorized individuals, may damage the reputation of the Ministry
Standards	i. All employees should not communicate official information via disposable emails like yahoo, gmail, etc. ii. Official communications must be done through Government Mailing System only.