MTWARA MIKINDANI MUNICIPAL COUNCIL

ICT POLICY

Prepared by:

Municipal Director
Mtwara Mikindani Municipal Council
Box 92,
MTWARA

May 2014

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

BS	Base Station
COSTECH	Commission for Science and Technology
CGI	Common gateway interface
CRT	Cathode Ray Tube
DC	Direct Current
DCC	District Council Committee
DDR-SDRAM	Double Data Rate Synchronous DRAM
DED	District Executive Director
DHCP	Dynamic Host Communication Protocol
DIS	Distributed Information System
DLP	Digital Light Processing
DMIS	Division of Management of Information System
DNS	Domain Name Service
DPI	Dot per Inch
DROMAS	District Roads Management System
EIDE	Enhanced Integrated Drive Electronics (ATA)
GFS	General Statistics Finance Codes
GPSA	Government Procurement Services Agency
HP	Hewlett Parked
HQ	Head Quarter
Hz	Unit measure of Frequency (Hertz)
ICMP	Internet Control Message Protocol

ICT	Information Communication Technology
IDE	Integrated Drive Electronics
IEC	International Electronic Commission
IEEE	The Institute of Electrical and Electronics Engineers
IMAP	Internet Message Access Protocol
ISO	International Standard Organization
ITN	Independent Telecommunication Network
ITU	International Telecommunication Union
LACP	Link Aggregation Control Protocol
LCD	Liquid Crystal Display
LGA	Local Government Authority
LGMD	Local Government Monitoring Database
MB	Megabytes
MCST	Ministry of Communication, Science and Technology
MDIX	Medium Dependent Interface Crossover
MDAs	Ministries Departments and Agencies
MIS	Management of Information System
MS-Office	Microsoft Office.
NAT	Network Address Translation
NTP	Network Timing Protocol
PABX	Private Automatic Branch Exchange
PAT	Port Address Translation

PCI	The Peripheral Component Interconnect
PDF	Portable Document Format
PCL	Printer Command Language
TIFF	Tagged Image File Format
PE	Personal Emoluments
PlanRep2	Planning and Reporting Tool
PM	Preventive Maintenance
POP	Post Office Protocol
RAID	Redundant Array of Independent Disk technology
RAM	Random Access Memory
RCC	Regional Council Committee
RPC	Remote procedure call
RS	Regional Secretariat
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SP	Service Pak
SQL	Structural Query Language
SSH	Secure Shell Protocol
TCO	Total cost of ownership
TCRA	Tanzania Communication Regulation Authority
TE	Terminal Equipment
TFT	Thin Film Transistor

TMIS	Transport Management Information System
UCC	University Computing Centre
UPS	Uninterruptible Power Supply Unit
US FCC	The United States Federal Communications Commission
USB	Universal Serial Bus
URT	United Republic of Tanzania
VA	Volt-Ampere
VPN	Virtual Private Network
WXGA	Wide screen Resolution
MC's	Municipal Councils
LAN	Local Area Network
TTCL	Tanzania Telecommunications Company limited

GLOSSARY

Adapter Any hardware device that allows communications to occur through physically dissimilar systems. This term usually refer to peripheral cards that are permanently mounted inside computer's bus to another medium such as a hard disk or a network.

Ad-hoc Networks are the simplest form of wireless network created by two or more wireless enabled computers communicating with each other directly. These types of WLANs are useful for creating small dynamic networks.

Backup The process of writing all the data contained in online mass – devices to offline mass storage devices for the purpose of safekeeping. Backups are usually performed from hard disk drives to tape drives. Also referred to as archiving.

Bluetooth this is a low-cost radio solution that can provide links between devices. Originally, and more typically the range of these devices is up to 10 meters. Bluetooth has access speeds of up to 721 Kbps.

CPU (Central Processing Unit) The main processor in a computer

Database is a collection of information that is organized so that it can easily be accessed, managed, and updated. This can be manual or computerized.

Domain In Microsoft networks, an arrangement of client and server computers referenced by specific name that shares a single security permission database. On the

Internet, domain is a name collection of hosts and sub domains, registered with a unique name by the inter NIC (Network Interface Card).

Domain Name System (DNS) The TCP/IP network service that translates fully qualified domain names (host names) into IP address.

Dynamic Host Configuration Protocol (DHCP) A method of automatically assigning IP addresses to client computers on a network.

File Transfer Protocol (FTP) - A simple Internet protocol that transfers complete files from an FTP server to client running the FTP client. FTP provides a simple, low overhead method of transferring files between computers but can not perform browsing functions. Users must know the URL of the FTP server to which they wish to attach.

Hypertext Mark-up Language (HTML) A textual data format that identifies sections of a document such as headers, lists, and hypertext links and so on. HTML is the data format used on the World Wide Web for the publication of Web pages

HTTP (Hyper Text Mark-up Language) An Internet protocol that transfers HTML documents over the Internet and responds to context changes that happen when a user clicks a hyperlink.

Information and Communication Technologies (ICT) – Is a generic term used to express the convergence of information technology, broadcasting and communication. One prominent example is the Internet.

Information Technology (IT) – Embraces the use of computers, telecommunications and office systems technologies for the collection, processing, storing, packaging and dissemination of information.

Local Area Network (LAN) – A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

Physical port A serial (COM) or parallel (LPT) port that connects a device such as printer directly to a computer

Simple Message Transfer Protocol (SMTP) An internet protocol for transferring mail between Internet hosts. SMTP is often used to upload mail directly from client to an intermediate host, but can only be used to receive mail by computers connected to the internet.

Wide Area Network (WAN) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

Wi-Fi LAN (WLAN) A wireless local area network (WLAN) is two or more computers joined together using radio frequency (RF) transmissions. This differs from a wired LAN, which uses cabling to link together computers in a room, building, or site to form a network.

TCO is defined as the total cost of a good or service throughout the life of utilizing the good or service and includes both initial or acquisition costs as well as recurring costs.

EXECUTIVE SUMMARY

This Policy applies to all Users of IT Systems, including but not limited to Mtwara Mikindani Municipal Council staff. It applies to the use of all IT Systems. These include systems, networks, and facilities administered by Mtwara Mikindani Municipal Council, as well as those administered by individual departments, and other Mtwara Mikindani Municipal Council -based entities.

Use of IT Systems, even when carried out on a privately owned computer that is not managed or maintained by Mtwara Mikindani Municipal Council, is governed by this Policy.

Policy Statement

The purpose of this Policy is to ensure an Information Technology infrastructure that promotes the basic missions of the Mtwara Mikindani Municipal Council in learning, and administration. In particular, this Policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of IT Systems;
- To ensure that use of IT Systems is consistent with the principles and values that govern use of other Mtwara Mikindani Municipal Council facilities and services;
- To ensure that IT Systems are used for their intended purposes; and
- To establish processes for addressing policy violations and sanctions for violators

Reason for the Policy

Information Technology ("IT"), the vast and growing array of computing and electronic data communications facilities and services, is used daily to distribute material in multiple media and formats. Information Technology plays an integral part in the fulfillment of Mtwara Mikindani Municipal Council communication, administrative, and other roles. Users of Mtwara Mikindani Municipal Council's IT resources have a responsibility not to abuse those resources and to respect the rights of the members of the community as well as the Mtwara Mikindani Municipal Council itself. This Mtwara Mikindani Municipal Council Information Technology Appropriate Use Policy provides guidelines for the appropriate use of Mtwara Mikindani Municipal Council's IT resources as well as for the Mtwara Mikindani Municipal Council's access to information about and oversight of these resources.

Most IT use parallels familiar activity in other media and formats, making existing Mtwara Mikindani Municipal Council policies important in determining what use is appropriate. Using electronic mail ("email") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. Mtwara Mikindani Municipal

Council policies that already govern freedom of expression and related matters in the context of standard written expression govern electronic expression as well. This Policy addresses circumstances that are particular to the IT arena and is intended to augment but not to take over from other relevant Mtwara Mikindani Municipal Council policies.

CHAPTER ONE

1.0 BACKGROUND

1.1 Introduction

This is the First ICT POLICY for Mtwara Mikindani Municipal Council. this regard, there was need to prepare ICT POLICY to guide the Municipal Council to deal with critical issues in ICT Infrastructures in Mtwara Mikindani Municipal Council and to guarantee the improvement in service delivery in the Municipal Council.

The ICT POLICY covers a Growing of ICT Infrastructures in Mtwara Mikindani Municipal Council. The ICT POLICY stipulates the Municipal Council's Vision and Mission statements, Core operational functions, Objectives, strategies to achieve those objectives that the Council is expected to achieve. This ICT POLICY will smoothen the process of delivering services through ICT Unit infrastructure in Mtwara Mikindani Municipal Council in general.

1.2 Vision, Mission statements

Mtwara Mikindani Municipal Council ICT Policy is aligned to the following Vision statement.

1.2.1 Current Vision

"An accountable Council which is capable of providing quality and sustainable services," and;

1.2.2 Current Mission

The Mission statement was "*To facilitate the provision of social and economic services through involvement of stakeholders".*

1.3 Municipal Council Objectives

In attaining the above Vision and Mission statements, the Municipal Council had the following seven objectives:

a. Improved services and reduced HIV/AIDS infection rates.
b. Enhanced, sustained and effective implementation of the National Anti-Corruption Strategy.
c. Improved access and quality of social services.
d. Economic services and infrastructures in terms of quality and quantity improved.
e. Good governance and administration enhanced.
f. Social welfare, gender and community empowerment enhanced.
g. Emergency preparedness and disaster management improved.

1.4 Core operational functions

In response to the above objectives, the Municipal Council in the past five years developed core functions which were distributed to the respective departments and units as follows:-

a. Develop quality infrastructures and urban human settlements.
b. Promote pre- primary, primary, secondary and adult education.
c. Promote quality agriculture and livestock keeping.
d. Supervise and ensure provision of quality health services to the community.
e. Construct, strengthen and ensure that all roads are passable throughout the year.
f. Promote and ensure good governance.

g. Promote Community participation and ensure sustainable cooperatives in a competitive environment.

h. Fight the spread of HIV/AIDS.

i. Develop an environment of gender equity and equality.

j. Ensure sustainable natural resources and environmental management.

CHAPTER TWO

2.0. POLICY DEVELOPMENT

This Policy may be periodically reviewed and modified by the Municipal Director, who may consult with relevant Mtwara Mikindani Municipal Council committees, departments/clusters, and staff.

2.1. Internal Auditor

The Head of Internal Audit shall audit the IT Unit of the Council and ensure compliance With the Mtwara Mikindani Municipal Council's ICT Policy.

2.2. POLICY SECTIONS

2.2.1. Appropriate use of IT Systems

Although this Policy sets forward the general parameters of appropriate use of IT Systems, departments and staff should consult their respective governing policy manuals for more detailed statements on permitted use and the extent of use that the Mtwara Mikindani Municipal Council considers appropriate in light of their varying roles within the community. In the event of conflict between IT policies, this Appropriate Use Policy will succeed.

a) **Appropriate Use**. IT Systems may be used only for their authorized purposes -- that is, to support the research, administrative, and other functions (IFMS) of Mtwara Mikindani Municipal Council. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User.

b. **Proper Authorization**. Users are entitled to access only those elements of IT Systems that are consistent with their authorization.

c. **Specific Proscriptions on Use**. The following categories of use are inappropriate and prohibited:

2.2.2 **Use that obstructs, interferes with, impairs, or otherwise causes harm to the activities of others**.

Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming"

(spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2.2.3 **Use that is inconsistent with** Mtwara Mikindani Municipal Council**'s non-profit status**.

The Mtwara Mikindani Municipal Council is a non-profit, tax-exempt organization and, as such, is subject to specific state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non- Mtwara Mikindani Municipal Council purposes is generally prohibited, except if specifically authorized and permitted under Mtwara Mikindani Municipal Council conflict-of-interest, outside employment, and other related policies.

Use of IT Systems in a way that suggests Mtwara Mikindani Municipal Council endorsement of any political candidate or ballot initiative is also prohibited. Users must abstain from using IT Systems for the purpose of lobbying that brings Mtwara Mikindani Municipal Council involvement

2.2.4. Use damaging the integrity of Mtwara Mikindani Municipal Council **or other IT Systems**.

This category includes, but is not limited to, the following six activities:

a) **Attempts to defeat system security**. Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking" or guessing and applying the identification or password of another User.

b) **Unauthorized access or use**. Mtwara Mikindani Municipal Council recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that user.

c) **Disguised use**. Users must not hide their identity when using IT Systems, except when the option of anonymous access is explicitly

authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

d) **Distributing computer viruses**. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

e) **Modification or removal of data or equipment**. Without specific authorization, Users may not remove or modify any Mtwara Mikindani Municipal Council -owned or administered equipment or data from IT Systems.

f) **Use of unauthorized devices.** Without specific authorization, Users must not physically or electrically attach any additional device (such as an external disk, printer, or video system) to IT Systems.

2.2.5. **Use in violation of law. Illegal use of IT Systems**.

That is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography.

2.2.6. **Use in violation of** Mtwara Mikindani Municipal Council **contracts**.

All use of IT Systems must be consistent with the Mtwara Mikindani Municipal Council 's contractual obligations, including limitations defined in software and other licensing agreements.

i. **Personal Account Responsibility**. Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any User changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator

ii. **Encryption of Data**. Users are encouraged to encrypt files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks

iii. **Personal Identification**. Upon request by a Systems Administrator or other Mtwara Mikindani Municipal Council authority, Users must produce valid Mtwara Mikindani Municipal Council identification.

CHAPTER THREE

3.0. CONDITION FOR MTWARA MIKINNDANI MUNICIPAL COUNCIL ACCESS

3.1.1. Conditions.

In accordance with state law, the Mtwara Mikindani Municipal Council may access all aspects of IT Systems, without the consent of the User, in the following circumstances:

a. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems; or

b. When required by state, or local law or administrative rules; or

c. When there are reasonable grounds to believe that a violation of law or a significant breach of Mtwara Mikindani Municipal Council policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or

d. When required to preserve public security/safety.

3.1.2. Process: MTWARA MIKINDANI MUNICIPAL COUNCIL.

Through the Systems Administrators, will log all instances of access without consent

3.1.3. User access deactivations.

In addition to accessing the IT Systems, the Mtwara Mikindani Municipal Council, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the User of any such action.

3.1.4. Encrypted material.

Encrypted files, documents, and messages may be accessed by the Mtwara Mikindani Municipal Council

4.0. ENFORCEMENT PROCEDURES

4.1.1. Penalties.

Individuals found to have violated this Policy may be subject to penalties provided for in other Mtwara Mikindani Municipal Council policies dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Systems Administrator.

4.1.2. Legal Liability for Unlawful Use.

In addition to Mtwara Mikindani Municipal Council discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

4.1.3. Appeals.

Users found in violation of this Policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

5.0. MANAGEMENT OF ICT RESOURCES.

Management of all IT resources of the Council shall be under the supervision of Head of IT Unit. This Section provides guidelines on Management of IT resources.

5.1.1 Hardware

All hardware devices acquired for or on behalf of Council or developed by Council employees or contract personnel on behalf of Council are and shall be deemed Council property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

The following standards will be used for Council IT equipment (excluding test Computers) that are fully supported by the IT Unit.

5.1.2. Server's standards

i. Servers will be installed and maintained in the designated Server room that meet Proven standards
ii. Servers will be based on Intel Processor and their specifications will be reviewed regularly in line with business requirements and technological development
iii. Mission critical servers shall be enterprise-class rack mountable and shall be installed in the server room.
iv. Rack mountable mass storage units shall be used for database, data and files Storage
v. Minimum specifications shall be reviewed yearly and specified according to requirements but shall not be below entry levels in respective class.
vi. High-autonomy UPS (such as APC 750) shall be used to protect the Servers.

5.1.3. PC and Laptop standards

i. Desktops personal computers will be provided to employees who work primarily from the office.
ii. Laptop will be provided to employees who work primarily from the field.
iii. All desktop computers and laptops shall be based on Intel latest processors or equivalent Intel compatible processors and shall not be cloned computers.
iv. All PCs shall meet the Council minimum specification requirement.
v. All desktops computers shall be powered by UPS and laptop protected by electric surge protector.
vi. Laptops will be provided to employee with appropriate security locks. Such as Password and software like folder lock.

5.1.4. Monitors

i. Monitors will be provided for both desktop and laptop systems.
ii. Standards monitors will be Flat panel 17-inch or above monitor, depending on job requirements.

The recommended Monitor is Flat type Liquid crystal Display (LCD) and not Cathode ray display because of the health reason and latest technology.

5.1.5. Printers

i. All Employees will be given access to appropriate network printers.
ii. In some limited cases, employees may be given local printers if deemed necessary by the Head of IT Unit.
iii. Employees needing computer hardware other than what is stated above must request such hardware from the IT Unit. Each request will be considered on a case by-case basis in conjunction with the Public procurement regulations.

5.1.6. Hardware from outside

i. Equipment not owned by the Council shall not be plugged into the Council network without permission from the Head of IT Unit.
ii. Equipment not owned by the Council shall not be brought into and/or used within the Council's premises without permission from the Head of IT Unit.

5.1.7. Stolen or Lost of ICT Equipment

i. When employee's ICT equipment stolen or lost, must report the event in writing to Head of IT Unit through his head of Department for further action.
ii. In reporting stolen or lost of ICT equipment, the affected employee shall complete a specific form in this regard.
iii. When employee transferred from Mtwara Mikindani Municipal Council shall return all ICTs resources including Laptop by filling special form prepared by head of ICT Unit.

CHAPTER FOUR

6.0. LOGICAL SECURITY.

This Section is set to ensure that the Council's data and Information is safeguarded against any kind of loss. It establishes rules relating to physical and data protection, data backup and restoration of data, virus infections and unauthorized access to systems by third parties.

6.1.1 Virus protection.

The IT specialist in an organization will maintain, detect, and prevent virus in the system, and make sure that anti-virus software protection is maintain on their machine.

6.1. 2.Software protection.

The IT Specialist must ensure that all software installed in an organization is complying with copyright Act, Always make sure that all software used in organization is authorized product.

6.1.3. Data protection.

The IT Specialist should protect data in an organization by creating strong user authentication, and encrypting data so that can

be seen by authorized user. . The organization should provide different access to different user in an organization by creating access account .Example access to server is only provided to Information system manager.

6.1.4. Multimedia internet security.

The IT specialist should install software which can view detail about all of the computers connected in the same router in organization server. These will make sure that all user of internet in organization to be seen, also install software which restrict user in use of internet.

6.2. PHYSICAL SECURITY.

The organization should make sure that all IT Resources found within an organization are well protected so as to prevent access to, interface with or damage to information asset.

i. Management shall ensure that all software, information and data generated, gathered or stored in the Council's Information assets are protected against theft, disclosure, leakage, piracy and destruction.
ii. Users shall not disclose their passwords. Any user who detects an act by any person to obtain a password other than his/her shall report the incident to his Head of Department for appropriate action.
iii. Any loss of information contained in IT equipment shall be reported in writing to the Head of Department for appropriate action.
iv. Users shall not access any information other than what they are specifically authorized to.

6.2.1. Fire.

Guidelines for fire control;

- Fire extinguishers must be located in an organization where IT Resources found, and all organization staff should be trained on how to use fire extinguishers.
- In case of data and information security against fire, the copy of data and information in an organization should be taken and stored outside the organization (making backup of the system data and information.)

6.2.2. Smoke.

Guidelines for smoke control;

- Smoking in an organization must be restricted so as to protect rooms having IT equipment.
- Smoking warning must be placed in wall of an organization.
- Smoke detectors may be installed in an organization

6.2.3. Dust.

Guidelines for Dust control;

- All rooms which contain IT equipment must be kept clean always.
- Computers and other equipment must be covered after using them.
- Dust must be blown from Computer before using computer and other hardware in organization.

6.2.4. Humidity.

Guidelines for humidity control;

- IT equipment should well be protected from contact with water, therefore an organization should prepare conducive environment for placing IT system.

6.2.5. Temperature Extremes.

Normally IT Systems should be kept between 10c and 32c temperature.

Guidelines for temperature control;

- IT equipment documentation should be read to see which temperature range will be satisfactory.
- IT equipment should not be placed to wall, which can interface with air condition fluctuations.

6.2.6. Disposer protection.

The organization should make sure that all used resources in IT system are placed together, and send back to their industries for recylering.

Guidelines for disposer control;

- All used compact disk that expired are returned to industries for recycling.
- All computers which are not corresponding with the existing technology should be kept in store room.
- Used printer ink must be recycled.

6.3. PREVENTING ACCIDENTS.

The IT system can essay cause an accident so an organization should make sure that always the system is safe from environment problems.

6.3.1. Food and Drinks.

Guidelines for Food and Drinks control;

- Eating and drinking in IT equipment room is prohibited in an organization.

6.4. ANTIVIRUS MEASURES

i. Peer folder-sharing should be discouraged and whenever needed, they should be properly secured with assistance from the IT Unit.
ii. Users are not allowed to share, exchange or use external storage devices such as diskette, CDs, DVDs, flash disks and external hard disks containing data obtained from outside the Council unless the exchange has been authorized.
iii. The IT Unit must ensure that all data storage equipment taken outside the Council is checked for virus prior to using them again on the network.
iv. Users shall forward any virus warnings or alert of any kind to the IT Unit.
v. Users shall delete any suspicious email (spam, chain and junk) from unknown or suspicious sources.
vi. All Computers, Laptop, Servers of the Council shall use licensed Software such as Ant-viruses.

6.3.1. Data Backup and Restoration

i. Systems and data backup must be performed daily, weekly and monthly in a manner that will ensure no loss in the event such backed-up data are required.
ii. Backup storage of the same data must be done on two separate media and stored in physically separate locations to be specified by the IT Unit.
iii. Users shall be assisted by the IT Unit to backup their individual information in their respective computers at least once every month.
iv. The IT Unit must ensure that all strategic information systems are stored in the Server and are backed up regularly.

6.3.2. Internet Browsing

i. Users will be responsible and liable for their activities on the Internet.
ii. The Council reserves the right to inspect, monitor, filter and disclose the content of any Internet utilization. This may include visited IP addresses and websites. Prior notice shall be given to the Users.
iii. All browsing on the Internet should ensure Council's interest is higher than Users.
iv. Browsing of Pornographic sites is prohibited.
v. Users are not allowed to install software downloaded from Internet.

vi. Users are advised not to accept "**Remember your password"** feature or message resulted from logon authentication since this poses risks of further access to the system by unauthorized users

vii. Users shall not use unauthorized chat rooms, chat channels or browse and play online computer games.

6.3.3. Email

i. Application for an email account must be made through specified form.

ii. Use of the Council's email system for personal purposes is allowed provided it does not consume space unnecessarily and does not interfere with staff productivity. However users shall not use the same for personal commercial purposes, or facilitation of illegal activities of any kind.

iii. Employees shall not use Council's email system to create, send or forward information that contains obscene, threats or any other inappropriate content.

iv. Employees shall not send chain emails or mass emails addressed to large user groups.

v. Users must use extreme caution when opening e-mail attachments received from unsolicited senders, which may contain viruses and malicious codes.

vi. All official incoming emails should be directed to and handled by office of the Council Director.

vii. Official Email addressed to organizations or individuals outside the Council must clearly identify the user by full name, position and contact address in the Council.

viii. Emails shall bear standard disclaimer.

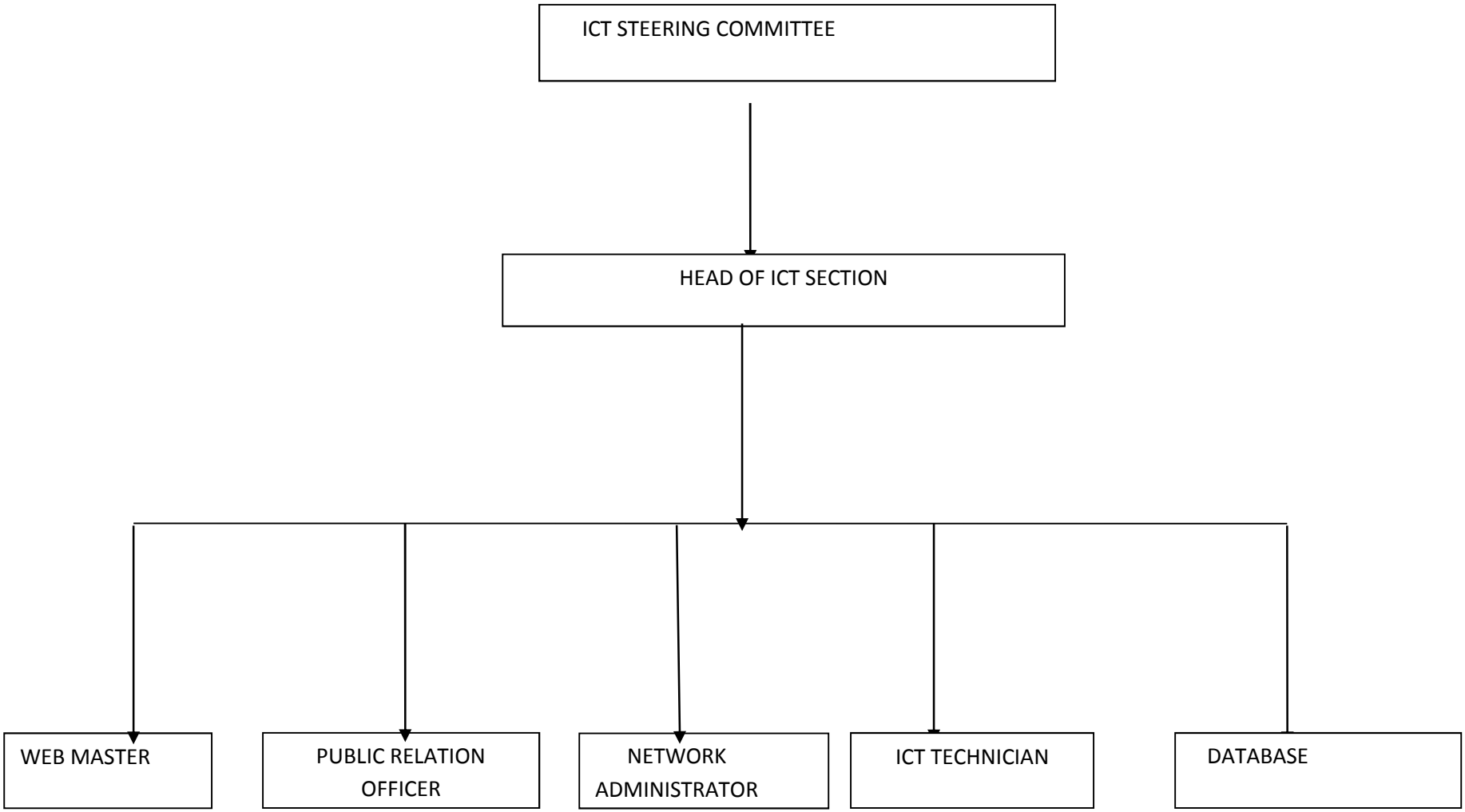
ix. The Council reserves the right to inspect, monitor and disclose the contents of any email created, sent, received or forwarded by using the Council computer networks or email system.

x. Users are prohibited to accept "Remember your password" feature or message resulted from logon authentication in order to avoid risk of future access to the system by unauthorized users.

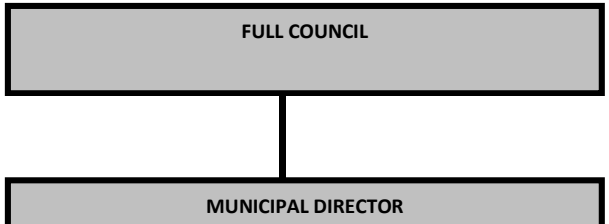
xi. All ongoing E-mail shall be in PDP format.

xii. Users shall access their respective Council mail account at least two (2) times per day to ensure timely handling of information.

APPENDIX 1: MTWARA MIKINDANI MC's ICT Organization Flow chart.



APPENDIX 2: MUNICIPAL COUNCIL ORGANIZATION CHART



Appendix 3: ICT STEEL COMMITTEE

ICT STEEL COMMITTEE
MTWARA MIKINDANI MUNICIPAL COUNCIL.

CHAIRPERSON: **MUNICPAL ECONOMIC PLANNING STATISTICS &MONITORING OFFICER**

SECRETARY: **COMPUTER SYSTEMS ANALYST (ICT)**

MEMBERS:

1. **MUNICIPAL TREASURE FINANCE&TRADE (MT)**
2. **MUNICIPAL**
3. **MUNICIPAL MEDICAL OFFICER (MMO)**
4. **MUNICIPAL TOWN PLANNING OFFICER (MTPO)**
5. **MUNICIPAL HUMAN RESOURCE OFFICER (MHRO)**
6. **MUNICIPAL ENGINEER (ME)**

Appendix 4: PREPARATION, REVIEW ANDA APPROVAL

Prepared by:	**Reviewed by:**
Ally A. Ndale	**Magnus Kisweka**
Acting Head ICT Unit	**Acting Municpal Economic Planning Statistics & Monitoring Officer**
Mtwara Mikindani Municipal Council	**Mtwara Mikindani Municipal Council**
P.O. Box 92,	**P.O. Box 92,**
MTWARA	**MTWARA**
Signature…….	**Signature…….**
Date……	**Date……..**

Approved by:

…….

(Shimwela L,E,S)

Municipal Director

Mtwara Municipal Council

Date…….