ARUSHA MUNICIPAL COUNCIL

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

FOR

THE ARUSHA MUNICIPAL COUNCIL

MAY 2011

EXECUTIVE SUMMARY

This document describes an Information Communication Technology (ICT) Policy for the Arusha Municipal Council (hereinafter referred to as "AMC" or "the Municipal"). The Policy lays down general guidelines and framework for the use and management of the Municipal's ICT resources.

In formulation of this Policy, the Municipal has drawn experience from the **National ICT Policy** and other comparable organizations and has made reference to the international best practices in Information Communication Technology (ICT). Views from the Municipal's employees have also been accommodated.

The primary objective of this Policy is to ensure that all ICT resources and systems of the Municipal are implemented and operated in a manner that does not compromise security, integrity, confidentiality and continual availability of systems, information or data. Accordingly, the Policy outlines key requirements in respect of the following major areas:

(i) Acceptable Use and Ownership of data;
(ii) Procurement of ICT Equipment and Distribution;
(iii) Information System Use;
(iv) Information Security;
(v) Web-applications;
(vi) Web-site Management;
(vii) Internal and external communications;
(viii) ICT Resources Management;
(ix) Monitoring and Evaluation of the Policy; and
(x) Policy review.

The Policy outlines the duties and responsibilities of various stakeholders (including users) of the Municipal's ICT resources.

The Municipal will endeavour to ensure that the users of the Municipal's ICT resources are kept abreast of new development and advancement in ICT, the risks that the Municipal's ICT resources continue to be exposed to, and the available risk mitigation initiatives that need to be applied. The Municipal will carry out regular assessment of status of users' compliance with the requirements of the Policy. An implementation status report will be prepared pursuant to each assessment exercise and necessary corrective action taken by the Municipal.

In order to ensure that the Policy remains effective and relevant to the Municipal and its stakeholders, the Policy will be reviewed and updated after every one year or at shorter intervals as circumstances may dictate.

Users of the Municipal's ICT resources are called upon to familiarize themselves and fully comply with the requirements of this Policy.

TABLE OF CONTENTS

GLOSSARY

In this Policy, unless the context otherwise requires, the following meaning of words and phrases shall apply:

Word(s)	**Meaning**
Access Controls:	Means of establishing and enforcing rights and privileges allowed to users.
Access Rights:	Authorized entry into a computer system to read, write, modify, delete or retrieve information contained therein.
Application Software:	Computer software designed to perform a defined business function.
Audit Trail:	A trailing mechanism on what was done, when, by whom and what was affected.
Authentication:	Mechanism of verifying the identity of user.
Authorization:	Enabling specification and the subsequent management of allowed actions for a given system. It relies on identification and authentication and enables access control.
Availability:	The assurance that information / data is available on a timely basis wherever / whenever it is needed to meet business requirements or to avoid substantial losses.
Full Council:	The municipal councilors' general meeting
Compliance:	To act according to certain accepted standards or rules.
Computer Network:	A collection of computers and devices Interconnected in order to enable resource sharing.
Confidentiality:	The protection of information from unauthorized disclosure.
Data Backup:	A process whereby data or programs in a computer are copied to storage media for possible future restoration.
Data Recovery:	A process of loading copied data or programs back into the computer from the storage media.
Data:	Basic facts and figures that can be processed to useful information.

Word(s)	**Meaning**
Database Administration:	The role generally associated with the management and control of a Database.
Database:	A collection of data that is organized so that its contents can easily be accessed managed and updated to serve multiple uses.
Division:	Means a directorate/unit as described in AMC's Organizational structure.
Email System:	All means of sending, receiving and storing electronic mails (e-mails).
Employee:	A person employed by the Municipal on permanent or contractual terms.
Encryption:	Conversion of messages (data / voice / video) into a form that cannot be understood by unauthorized readers.
End user:	All Users of ICT systems including Systems developers and Administrators.
Guidelines:	Acceptable approach in implementing a policy or procedure.
Head:	An officer in-charge of a Division.
ICT Equipment:	Tangible computer assets, such as computer Hardware, network or communication devices including laptops, personal computers, servers, printers and scanners, firewalls, digital cameras, modems, UPS
ICT Resources:	ICT Equipment together with operating procedures manuals, user guides and computer output.
Identification:	The process of distinguishing one user, process or resource from another.
Information and Communications Technology (ICT):	A generic term used to express the Convergence of information technology, broadcasting and communications.
Information Security:	Means of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
Information System:	The term that encompasses all components required for the processing of information e.g. Applications, Databases,

Word(s)	**Meaning**
	Operating systems and Network components.
Information Technology (IT):	Embraces the use of computers, communication and office systems technologies for the collection, processing, storing, packaging and dissemination of information.
Information:	Processed data that provide useful meaning to the Municipal.
Integrity:	The protection of information / data from unauthorized, unanticipated or unintentional modification or deletion, or to be able to identify such action when it cannot be prevented.
Intel Processors:	A brand of computer processors from Intel Company.
Internet:	A publicly accessible network of networks connecting users and organizations worldwide.
Intranet:	It is a private version of Internet, normally involving a one organization with the main purposes of enabling information sharing.
Malicious codes:	A new breed of Internet threat that cannot be efficiently controlled by conventional antivirus software alone.
Management:	The Municipal's Management Team consisting of heads of divisions.
Mass Storage:	Device that can store large amounts of Information
Mass-mail:	Email sent to more than one recipient at a time.
Network Administration:	The role generally associated with the management and control of computer networks.
Network equipment:	Any devices that facilitate or enhance data communication and includes routers, switches, hubs, firewalls, switches and PABX.
Policy:	A statement by Management and approved by the Full Council on strategy and direction that identifies and defines specific areas of concern and states the organization's position.
Premises:	Municipal's buildings with its outbuildings, land and property registered in the name of, or leased by the Municipal.

Word(s)	**Meaning**
Procedure:	Detailed steps to be followed to accomplish a particular task or to achieve specific results.
Rack:	Standard device for holding ICT equipment in a stack.
Regulations:	Directives issued as a code of conduct.
Server:	A powerful computer used for centralized data storage and processing of data.
Software Development tools:	Software and tools used in system Development
Software piracy:	The utilization of software in violation of its licensing agreement.
Software utilities:	These are small computer programs that provide an addition to the capabilities provided by the operating system.
Software:	Computer programs including operating systems, applications, utilities and accompanying documentation.
Staff Regulations:	The Municipal Staff Regulations.
Standards:	Specified uniform use of tools, techniques and methods to implement a policy or procedure.
System Administration:	The role associated with the management and control of operating system and its associated hardware
System Integrity and Recoverability:	These are means that ensure that processing of information resources behave in an appropriate or predefined manner in accordance with business processes. Often this means providing mechanisms to detect, prevent and correct the unauthorized modification, insertion, deletion or replay of information.
Systems:	Computer Systems.
Third Party:	An individual or legal entity explicitly authorized by the Municipal, including consultants, contractors, vendors, agents, and personnel affiliated to them.
Users:	Include Municipal's employees, temporary workers, external contractors, consultants, external auditors or any other parties which entered into an agreement to provide a service to the Municipal and obtain access to Municipal's information

Word(s)	**Meaning**
	systems and use Municipal's systems.
Virus:	A computer program that can copy itself and infect a computer without permission or knowledge of the user, and often causes damages to systems or data.
Webmaster:	Person responsible for updating, designing, developing, marketing and maintaining website.

LIST OF ACRONYMS

Word	Meaning
CD	Compact Disc
DVD	Digital Versatile Disc
ICT	Information and Communication Technology
ISP	Internet Services Provider
IT	Information Technology
OEM	Original Equipment Manufacturer
CSA	Computer System Analyst
PABX	Private Automatic Branch Exchange
PC	Personal Computer
PMU	Procurement Management Unit
PPA	Public Procurement Act Cap 410
AMC	Arusha Municipal Council
UPS	Uninterruptible Power Supply
VPN	Virtual Private Networks

1 Introduction

1.1 Background

The extensive use of computers and other ICT equipment is an increasing facet of the effective provision of Arusha Municipal Council. Computers are widely used for administration purposes, for communications and increasingly tool for providing service to the citizen. ICT systems represent a powerful facility for the enhancement of productivity and services, but can be vulnerable to accidental or deliberate misuse. This Policy sets out the Arusha Municipal Council guidelines on the use of ICT systems and the consequences of failure to comply with the Policy.

The Policy applies to all the Arusha Municipal Council employees, contractors, consultants, agents and any other persons who at any time use or have access to email or files, software applications and the internet during the course of their employment or business dealings with the Arusha Municipal Council, whether such use takes place on the Arusha Municipal Council premises or elsewhere.

The purpose of this policy is to set forth policies and guidelines for use of Arusha Municipal Council Computers and access to Files, Email and Internet systems by the users of the system.

There are various reasons for the need of such a policy/guideline, for instance:

A good policy protects both the employer and employee from misuse of Files, Applications, the internet, email and other electronic interfaces that might develop in the future. With the rapid evolvement of the internet and related systems there has been

enough scope for misuse to grow and build-up without adequate procedures being put in place to regulate acceptable behavior.

In putting into place a policy, the Arusha Municipal Council needs to take into account its own goals and burdens (financial and otherwise), whilst considering the needs and expectations of employees.

It must be clearly understood that it is the intent of the Arusha Municipal Council to protect itself and the employees from misuse of Arusha Municipal Council time and property. This ensures that misuse of the system is a deliberate choice by an individual and not due to lack of knowledge regarding procedures and policies. The consequence that such action by a user might lead to should be unambiguous to all concerned.

The aim of the policy is not to be restrictive, but to assist employees to be successful and valuable corporate citizens. However, users have to

Realize that their private actions on the system might be confused with those of the employer. Therefore, the consequences of the association between the Arusha Municipal Council and the user could and should not be allowed to be detrimental to the Arusha Municipal Council.

1.2 Vision, Mission, Functions of AMC

1.2.1 Vision

The vision of the arusha municipality is **"Arusha Municipal council with a growing and sustainable economy"**

1.2.2 Mission

The mission of Arusha Municipality is "to create a conducive environment for economic development, quality social services and sustainable environmental management"

1.2.3 Functions

i. To provide economic development support services in order to build increased expertise in Social and economic development as well as environmental conservation.
ii. To improve social sector services in order to enhance proper utilization of resources as a means of eradicating/eliminating poverty.
iii. To strengthen and promote social economic development in both rural and urban areas in accordance with the stipulated regulations.
iv. To collect adequate revenue which is satisfactory in provision of essential services to residents
v. To assist in building management capacity toward experts and village/mitaa leaders.
vi. To facilitate technical training to council experts at lower levels of local government [ward, village] so as to raise their performance and efficiency.
vii. To provide training to councils top management in order to build their capacity to deliver improved and adequate services to the people.
viii. To provide council experts with appropriate and adequate working gear and other required, facilities.
ix. To have in place and implement strategies and other mechanisms to raise adequate resources for service delivery in collaboration with other stakeholders.
x. To provide efficient administrative service to the management staff and deal with administrative issues and problems from the wards, Institutions and the general public.

2 Policy Objectives, Roles and Responsibilities

This Policy lays down general guidelines and framework for the use and management of the Municipal's ICT resources. It spells out the do's and don'ts in the use of the Municipal's ICT resources. All Users are obliged to read, understand and internalize this Policy for the purposes of complying with the set requirements.

2.1 Objectives

The primary objective of the policy is to ensure that all Information Communication Technology resources and systems of the Municipal are implemented and operated in a manner that does not compromise security, integrity, confidentiality and continual availability of systems, information or data.

2.2 Roles and Responsibilities

Various players have roles and responsibilities in formulation, approval and implementation of this policy. These include the Municipal Director, ICT Streering Committee, Management, Head of ICT unit and other users of ICT systems of the Municipal.

2.2.1 Municipal Director

The Municipal Director shall:

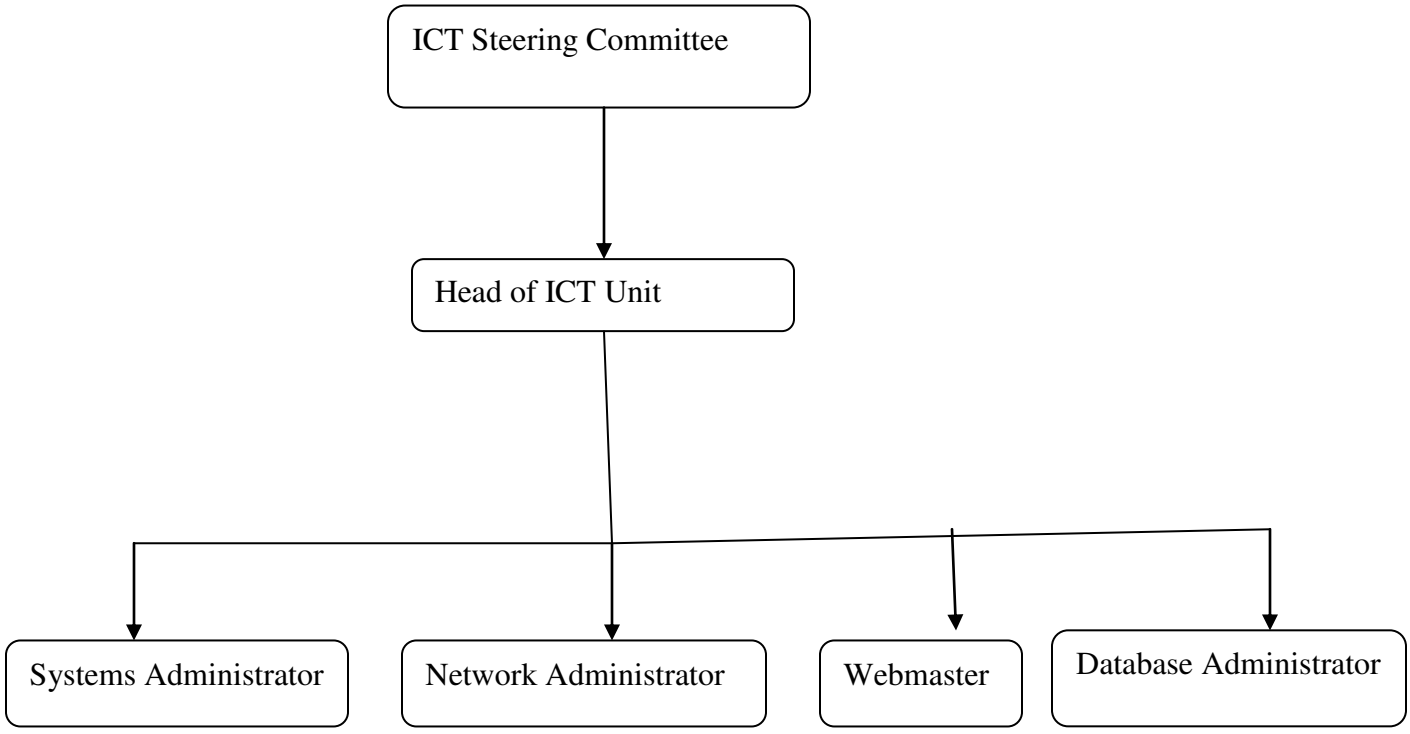
i. In consultation with the Head of IT Unit appoint a committee (hereinafter referred to as "ICT Steering Committee") and determine its terms of reference;
ii. recommend to the Management an appropriate ICT Policy for the Municipal; and
iii. Ensure the implementation of the policy.

2.2.2 Municipal Management Meeting (MMT)

Municipal Management Meeting shall: -

i. shall review and approve the ICT Policy and provide strategic directives on utilization of ICT in order to enhance productivity by ensuring effective and efficient systems.
ii. ensure that all Users under their supervision are aware and comply with the Policy;
iii. provide adequate and appropriate protection to ICT assets and resources under their control;
iv. ensure availability, integrity and confidentiality of information produced by systems under their areas of functional responsibilities, and thereby ensure continuity of operations; and
v. review and approve procedures, standards, rules and guidelines developed from this Policy for the purposes of maintaining business continuity and security of the Municipal's ICT resources.

2.2.3 ICT Organization structure



2.2.4 ICT Steering Committee

Responsibilities of the Committee shall include to:

i. propose AMC's ICT Policy for approval by management;
ii. coordinate the establishment and continued review of AMC's ICT Policy and Strategy;
iii. ensure that the ICT strategy is aligned with AMC's Plans;
iv. advise the Municipal Director in making considered decisions about the focus of ICT resources;
v. review all ICT services and applications including Municipal's website and infrastructure, with the view to advise the Municipal on required improvements; and
vi. ensure that the risks associated with ICT are managed appropriately.

2.2.5 Head of IT Unit

Subject to general oversight of the Municipal Director, the Head responsible for ICT shall oversee the overall administration of the Policy; and in particular, he/she shall: -

i. coordinate the review and amendment of the policy, as and when required in order to accommodate new technologies or services, applications, procedures, perceived dangers;
ii. plan and develop ICT security strategies;
iii. monitor adherence to the ICT Policy and the presence of potential threats and risks by conducting periodic ICT security reviews;
iv. keep abreast of ICT Security developments in respect of the ICT industry in general, and the Municipal's systems in particular;
v. initiate and recommend proposals to change, modify or improve the Policy; and
vi. recommend Procedures, Standards and Rules for effective implementation of the Policy.
vii. Overall in charge of the ICT function

2.2.6 Systems Administrator

i. Provides administrative and technical guidance to the users of information system at the Municipal
ii. Performs routine monitoring of servers
iii. Provides help desk services to systems users
iv. Provides systems users with different access level rights
v. Performs periodic backups and disaster recovery

2.2.7 Network Administrator

Overall administrator of the Municipal network

2.2.8 Database Administrator

i. Overall administration of database systems and supervision of data entry processes
ii. Develops and maintain formal procedures for data security, integrity and consistency in the cooperate database systems
iii. Performs routine monitoring of database

2.2.9 Webmaster

i. Develop and continually update the municipal's website

2.2.10 Head of Internal Audit Unit

The Head of Internal Audit shall audit the ICT Unit of the Municipal and ensure compliance with the Policy.

2.2.11 Users of IT Systems

All Users shall be responsible to safeguard ICT assets of the Municipal against all types of threats and alert Management of all vulnerable areas. Users shall also comply with all security controls set out in this Policy and other regulations of the Municipal.

This Policy, in its entirety shall be made available to all employees of the Municipal, who shall make themselves familiar with the relevant sections and sign a User Acceptance Form.

2.3 Compliance and Penalties

i. All Employees and other authorized Users of Municipal's ICT resources shall comply with the requirements of this Policy.
ii. The Head responsible for ICT shall enforce compliance by using audit trails on all IT resources used at the Municipal. In addition to ensuring compliance to this Policy, the audit trail shall be used to ensure, integrity and availability of information and services.
iii. Violations of this ICT Policy can lead to withdrawal and/or suspension of System and Network privileges and/or other disciplinary action to be determined by Management.

2.4 Management of IT resources

i. The Head responsible for ICT Unit shall be the custodian of all ICT resources of the Municipal including those centrally stored in the Server room.
ii. All Heads of Departments, Sections and Units shall be custodians of "Data and Information" for their respective places.
iii. All employees shall be custodians of all ICT resources allocated to them.

2.5 Asset Tracking / Inventory

All ICT related hardware/software are required to enter into Municipal ICT inventory within 3 days once purchased. The ICT inventory is kept by the ICT section, Accounts, and procurement. Municipal Director will require receiving the ICT inventory report whenever requested. ICT can inform the status of the assets to the department head, if he/she requires presenting to the report.

3 ACCEPTABLE USE AND OWNERSHIP OF DATA

3.1 Acceptable use

This Section is meant to protect users and the Municipal in general, from illegal or damaging actions by individuals.

i. All networking and computing systems and resources which include but not limited to Internet, Intranet, printing, software, storage media and network accounts for electronic mail or other access permission, are the property of the Municipal.

ii. ICT resources are to be used for purposes of advancing the Municipal's mandate. Inappropriate use of IT resources may expose the Municipal to risks including but not limited to loss of these resources, virus attacks and legal implications.

3.2 Physical and Systems Access

iii. Networking and computing equipment entrusted to Users must be secured against any threats.

iv. The Municipal's server(s) shall be kept in a secure server room.

v. All entries to the Server room must be recorded and security camera be installed to monitor all accesses.

vi. Desktop computers, laptop, scanners, printers and other peripheral equipment or systems under Users' custody must be handled with proper care to avoid damage, dusts etc.

vii. Computer application must be closed and Users must log off from the system when the system is not in use.

viii. All equipment must be switched off properly before Users leaves the office.

ix. Power protections on equipment must not be by-passed without proper authorization by Head of ICT Unit.

x. Users are not allowed to install hardware and personal software, including device drivers or change configurations on the Municipal's networking or computing systems.

xi. Users shall not allow non-AMC individuals to use ICT resources assigned to them without prior written authorization.

xii. All movement of ICT equipment must be authorized by Heads of Departments through a written form and the movement supervised by the Head of ICT Unit.

xiii. All computing and networking installations must be protected and made secure by the Municipal's ICT Unit. Problems related to installations or malfunctions must be reported to the ICT Unit.

xiv. Desktop computers, Servers and Laptops must be secured with password against unauthorized access by third parties.

3.3 Ownership of Data and Information

i. All Information and data processed, created, generated and stored in the Municipal's computer facilities shall remain the property of the Municipal.

ii. Any Department, Section or Unit within the Municipal that create any information or data shall be the owner of such information or data and shall be responsible for its integrity and confidentiality.

iii. No information shall be transferred, given or distributed to any organization or individual without authorization from the Municipal Director.

iv. All software created by the Municipal shall be the exclusive property of the Municipal, and shall not be transferred, given or distributed to any organization or individual without the written authorization of the Municipal.

v. All software Licensed to the Municipal shall not be transferred, given or distributed to any organization or individual.

4 PROCUREMENT OF IT EQUIPMENT AND DISTRIBUTION

This Section provides guidelines to the Municipal with respect to procurement and distribution of ICT resources. All ICT resources shall be procured in line with PPA Cap 410.

Procedures for planning, procurement, distribution, utilization and disposal of ICT resources for the Municipal are outlined hereunder.

4.1 Planning Acquisition

i. All User departments shall establish and submit, in writing, all applicable ICT requirements to the ICT Unit for procurement ahead of the next financial year.
ii. The ICT Unit shall consolidate all ICT requirements and submit them for inclusion in the budget for relevant financial year.
iii. Ad-hoc requirements from User Department, Section or Unit shall be forwarded to ICT Unit for procurement on the need-basis

4.2 ICT Resources entitlement

i. ICT resources will be allocated as per the Municipal plan and budget.
ii. Each Department, Section or Unit will be allocated ICT resources as per their requirements as determined and approved by Management.

4.3 Procurement of IT Resources

i. Specifications for procurement of ICT resources must be prepared taking into account Original Equipment Manufacturer (OEM) and reasonable warranty period.
ii. All procurement of ICT resources must be done in consultation with the ICT Unit.
iii. All software procured must be licensed and acquired from authorized software vendors. The procurement must include end-user training where applicable.

4.4 Lifetime and Replacement of ICT Resources

i. Replacement of ICT resources will be determined by system requirements, accompanied by a technical report by ICT Unit.

ii. Disposal of obsolete ICT resources and their corresponding replacement will be in line with applicable depreciation rate as contained in Municipal's financial Regulations.

iii. In disposal of obsolete ICT resources described under (ii) above, priority disposition shall be given to the employee(s) who was allocated the ICT equipment under disposal.

5 INFORMATION SYSTEM USE

This Section streamlines the use of information stored into different systems and utilized by Users in the course of their day-to-day operations.

Purpose of this Section is to allow control of access to the data and also to ensure appropriate access levels to different systems. It also establishes standards for creation of strong passwords, protection of such passwords and frequency of change.

5.1 Systems Access

i. Official request for access to the system must be made to the Head of IT Unit through the heads of Departments, Sections, Units and using specified forms, which shall specify the level of access.
ii. An employee's access to the system will be disabled during suspicious absence or as required by the departments responsible for administration.
iii. All activation of disabled access shall be re-applied though the specified form.
iv. Access to any system shall always be through the provided application software and under no circumstances should any End User by-pass the application software to access system data.
v. Software Utilities and tools that are not under Municipal's ownership shall not be used unless authorized by the ICT Unit.

5.2 User ID and Password

i. Passwords used shall not be based on personal information such as family names, (surnames, names of your children, spouse) years of birth, or login name.
ii. Passwords for the ICT resources must be discrete and alphanumeric, both upper and lower case characters (e.g., a-z, A-Z), have digits (0-9) and punctuation characters such as,!@#$ %^&*()_+|~-=\`{}[]:";'<>?,./)
iii. All user level passwords must be changed at least once every three (3) Months.
iv. User ID and Passwords must not be shared, availed or known to others including the ICT administrators and should not be written down or stored on-line.

v. Initial passwords shall immediately be changed prior to accessing the system.
vi. Users should not use the last three previous passwords.
vii. Password should have a minimum of eight (8) characters and should not contain words in any language, slang, dialect, or jargon.
viii. Password must be easy to remember but difficult to guess.

5.3 Use of the Available System

i. Management shall enforce usage of an ICT system once the system has been approved.
ii. Heads of department shall demand specific reports from systems in use from time to time as directed by Management.
iii. Management shall only accept system-generated reports in cases where applicable systems exist.
iv. Management must approve operating procedures to be used in all established systems.
v. Any user who discovers abnormalities, errors or loopholes in the system must report to the Head of ICT Unit.
vi. Users shall not access information they are not specifically authorized to.
vii. Users must not disclose, or disseminate to an unauthorized person, any information or data that they come across during their access of the system.
viii. Users shall ensure that any discarded information or data is properly destroyed.

6 INFORMATION SECURITY

This Section is set to ensure that the Municipal'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 Information Protection

i. Management shall ensure that all software, information and data generated, gathered or stored in the Municipal'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 ICT 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.
v. Users shall not disseminate any of the Municipal's information or data to unauthorized persons or organizations without the authorization of the Municipal Director.
vi. Users shall ensure that any discarded information or data is properly collected, stored and destroyed according to the procedures and guidelines on information destruction.
vii. Users shall regularly update their antivirus and the ICT Unit shall ensure that computers are installed with up-to-date versions of antivirus.
viii. Users shall ensure that all computers or information storage media to be discarded, disposed of, or sent outside the Municipal's premises for any purpose, have all the information or data removed from them.
ix. Users shall keep and store all the Municipal data and Information into the respective folder in the assigned network drives on the Servers, which will be backed up regularly.

6.2 Protection against Hazards

i. Power supply to the ICT equipment must be checked to ensure that it is available and safe for the equipment.
ii. Management must ensure that all ICT resources are protected against natural hazards including fire, floods and lightning.
iii. Server rooms must be protected against leakage and any kind of water.
iv. Smoke detectors must be installed on the server room.
v. Fire extinguishers must be installed on the server room and Users must be trained on how to use them.
vi. Fire drills must be conducted from time to time to ensure readiness in combating fire.

6.3 Physical Access to Servers and Server Room

i. Management must provide Server rooms that meet proven standards.
ii. Server rooms must not be accessible to unauthorized persons.
iii. Access to servers must bear prior written approval from the Head of ICT Unit.
iv. All administration to Servers computers shall be done remotely from computers other than the Server themselves unless it is extremely necessary.
v. Server rooms must have special measures against theft.

6.4 Data Backup

i. Systems and data back up 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 ICT Unit.
iii. Users shall be assisted by the ICT Unit to backup their individual information in their respective computers at least once every month.
iv. The ICT Unit must ensure that all strategic information systems are stored in the Server and are backed up regularly.
v. Management must provide resources to allow for disaster recovery procedures.

6.5 Data Restoration

i. Checks must be made at least every quarter to ensure that backups made are valid and that data can be restored.
ii. The ICT Unit must ensure that restoration procedures are tested using valid backups.

6.6 Antivirus Measures

i. The ICT Unit shall ensure that all computers are installed with authorized and licensed antivirus software, and the same is up-to-date and activated whenever the computer is in use.
ii. The ICT Unit shall ensure that all security patches are installed in all computers as recommended by software manufacturers.
iii. The ICT Unit shall ensure that all incoming and outgoing attachments on electronic mails are scanned for virus.
iv. The ICT Unit shall ensure that the Municipal network is protected by a firewall whose software is up to date.
v. Users shall not install and run any computer games on the Municipal's computers, to avoid virus infection.
vi. Peer folder-sharing should be discouraged and whenever needed, they should be properly secured with assistance from the ICT Unit.
vii. 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 Municipal unless the exchange has been authorized.
viii. The ICT Unit must ensure that all data storage equipment taken outside the Municipal is checked for virus prior to using them again on the network.
ix. Users shall forward any virus warnings or alert of any kind to the ICT Unit.
x. Users shall delete any suspicious email (spam, chain and junk) from unknown or suspicious sources.

6.7 Third Party System Support

i. ICT Unit should ensure that all software development tools that the third party system support requires are available and made available whenever required.
ii. Third Party System Support shall not work with their own equipment connected to the Municipal's network system.
iii. Third Party system support may be allowed to use their ICT tools for their work whenever it is extremely necessary. However their computers must be scanned for viruses before they are connected into the Municipal's computer network.
iv. Third Parties Systems Support is prohibited from copying any information or data from Municipal's systems to their storage devices.
v. All Third Party System Support shall sign confidentiality forms.
vi. All Third Party system support shall be given prior approval and supervised by ICT Unit.

6.8 Repair of Computers

i. The ICT Unit must ensure that all computers that require repairs outside the Municipal's premises are protected from unauthorized data access.
ii. In case of repair of Servers, all repairs must first be done in-house and incase of the necessity for Servers to be taken outside the Municipal's premises, all hard disks must be removed from the computer and retained to ensure data protection.

6.9 Audit Trail

Audit trail must be activated for all Servers and must be checked on a regular basis.

7 WEB-BASED APPLICATION

This Section provides general guidelines on the Municipal's web-based applications with regard to information shared between the Municipal and third parties.

7.1 Access and Use

i. The Municipal through the ICT Unit shall grant relevant access rights and privileges to third parties.
ii. Third parties' access to the Municipal's web-based application will be through a VPN Client.
iii. Users shall always log off and close the web-based application when not using the system.
iv. Wrongly posted data to the Municipal's web-based applications by third parties shall immediately be reported to the Municipal.
v. Users ID and Passwords must not be shared availed or made known to others.
vi. Any abnormalities, errors or loopholes in the system must be reported to the Municipal ICT Unit.

8 WEBSITE

This Section establishes guidelines on handling the contents of the Municipal's Website and how and when the information should be updated.

8.1 Website management

i. AMC website is the property of the Municipal.
ii. The Municipal's ICT Committee shall be responsible for comprehensiveness and accuracy of all information on the Website.
iii. The Head of ICT Unit shall perform the duties of the webmaster for the Municipal's website.
iv. The Webmaster shall ensure that no unauthorized contents are published.
v. The webmaster will coordinate development and maintenance of the Website.
vi. All content for publishing on the website must be approved by the Municipal Director.
vii. The information on the website must be updated regularly as and when new content become available.
viii. The Municipal's website shall bear standard disclaimer.

9 COMMUNICATION POLICY

This Section establishes guidelines on internal and external communication by Municipal's employee through network services and outline acceptance use of the communication media.

9.1 Intranet

i. ICT Unit shall be responsible for publishing and Updating Information on the Intranet.
ii. All official communication within the Municipal including circulars and Internal Memos, shall be published on the Intranet
iii. All official information shall be passed through and approved by Head of Department before publishing them on Intranet.
iv. The information on the Intranet shall be updated /published immediately when available.
v. The Municipal reserves the right to monitor and filter information prior to publishing.
vi. All employees must access the Intranet at least twice a day to guarantee timely circulation of information.

9.2 Internet Browsing

i. Users will be responsible and liable for their activities on the Internet.
ii. The Municipal 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 Municipal'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 shall not use unauthorized chat rooms, chat channels or browse and play online computer games.

vii. 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.

9.3 Email

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

ii. Use of the Municipal’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 Municipal’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 Municipal Director.

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

viii. Emails shall bear standard disclaimer.

ix. The Municipal reserves the right to inspect, monitor and disclose the contents of any email created, sent, received or forwarded by using the Municipal 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. Users shall access their respective Municipal mail account at least two (2) times per day to ensure timely handling of information.

10 IT RESOURCES MANAGEMENT

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

10.1 Hardware

All hardware devices acquired for or on behalf of Municipal or developed by Municipal employees or contract personnel on behalf of Municipal is and shall be deemed Municipal property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.
The following standards will be used for Municipal ICT equipments (excluding test computers) that are fully supported by the ICT Unit.

10.1.1 Servers 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 computer room only
iv. Rack mountable mass storage units shall be used for database, data and files storage
v. Minimum specifications shall be reviewed each year and specified according to requirements but shall not be below entry levels in respective class.
vi. High-autonomy UPS shall be used to protect the Servers

10.1.2 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 Municipal 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

10.1.3 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.

10.1.4 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 ICT Unit.
iii. Employees needing computer hardware other than what is stated above must request such hardware from the ICT Unit. Each request will be considered on a case by-case basis in conjunction with the Public procurement regulations.

10.1.5 Hardware from outside

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

10.1.6 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.

10.1.7 Software

i. All software procured by the Municipal or developed internally shall be the property of Municipal.
ii. All software must be used in compliance with applicable licenses, notices, contracts, and agreements.

10.1.8 Licensing

All software by the Municipal shall be properly licensed. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, is not allowed as it is against prevailing national and international laws.

10.1.9 Software standards

The following list shows the standard suite of software installed on the Municipal computers (excluding test computers) that is fully supported by the Head of ICT Unit:

10.1.9.1 PC's environment

The PC's environment shall consist of the following:

i. Microsoft Windows XP Professional/Vista/7 (As current standard client operating systems)
ii. Microsoft Windows compatible messaging utility (Ms Outlook and Ms Outlook express)
iii. Office productivity applications shall be Microsoft Office 2003/2007/2010
iv. Microsoft Internet Explorer 6.0 or above
v. Adobe Acrobat Reader 8.0 or above

vi. WinZip 8.0 or above
vii. Latest and powerful Antivirus

10.1.9.2 Server environment

The Server environment shall consist of the following:-

i. Microsoft Windows Server 2003 or above
ii. Red Hat Linux version 9
iii. Microsoft Active Directory Service or LDAP compatible directory
iv. Linux or Microsoft based E-mail system
v. Web services: Internet Information Services (IIS) and Apache
vi. Database Management Systems (DBMS): MS SQL server and MySQL
vii. Latest Epicor software

10.1.9.3 Other Applications

Specialized applications other than office productivity applications shall be determined by Municipal's operation requirements. Department that require software other than those prescribed above should request the same from ICT Unit.

10.2 Business Resumption

The Municipal shall position itself to mitigate and resume operations after any kind of disruption, in line with its approved Business Continuity Management Strategy.

11 ICT GUIDELINES

The Municipal has developed guidelines to assist the implementation of this policy, and here is the list of the guidelines:-

i. Maintenance and Outsourcing;
ii. Disk and Data Sanitation; and
iii. Risk Mitigation.

12 MONITORING AND EVALUATION

Compliance to this Policy will be monitored and evaluated by the Head of IT Unit based on, including:-

i. automated auditing / monitoring mechanisms
ii. physical Inspections; and
iii. internal auditing findings.

13 POLICY REVIEW

This policy will be reviewed every one year, or following significant security breaches / incidents influencing changes to ensure that it remains appropriate.

APPENDICES

14 DECLARATIONS BY USERS

These declarations have been designed to certify that users acknowledge that they are aware of the Municipal's Information and Communication Technology Policy and agree to abide by their terms.

(Declaration By Municipal Employee)

I, _____ (Full name) acknowledge that the Municipal's ICT Policy Regulations have been made available to me for adequate review and understanding. I certify that I have been given ample opportunity to read and understand them, and ask questions about my responsibilities on them. I am, therefore, aware that I am accountable to all their terms and requirements; and that I shall abide by them. I also understand that failure to abide by them; the Municipal shall take against me appropriate disciplinary action or legal action, or both, as the case may be.

Signature: _____

Department: _____

Job Title: _____

Date: _____/_____/_____

15 DECLARATION BY THIRD PARTY

I, _____ of

_____

(name your company and full address) do hereby acknowledge that the Municipal has provided me with adequate time to review and understand its ICT Policy Regulations. I am therefore aware of its terms and requirements. I do hereby undertake, on behalf of my organization, regardless of my current employment status, to be responsible to, and abide by them. I also understand that any failure to abide by the Policy shall result in appropriate legal actions being taken against me or my organization, or both, my organization and myself, as the case may be.

Signature: _____

Job Title: _____

Date: _____/_____/___

16 WEBSITE DISCLAIMER

The information contained on this website is provided in good faith, and every reasonable effort is made to ensure that it is accurate and up to date. Accordingly, this information is provided 'as is' without warranty of any kind. The Arusha Municipal Council excludes all warranties, either express or implied (including but not limited to any implied warranties of merchantability, fitness for a particular purpose, satisfactory quality or freedom from hidden defects).

In no event shall the Arusha Municipal Council be liable for any damage arising, directly or indirectly, from use of the information contained in this website including damages arising from inaccuracies, omission or errors.

Any person relying on any of the information contained in this website or making any use of information contained herein, shall do so at its own risk. The Arusha Municipal Council hereby disclaims any liability and shall not be held liable for any damages including, without limitation, direct, indirect or consequential damages including loss of revenue, loss of profit, loss of opportunity or other losses. The information contained in this website may be changed or updated at any time without notice.

In addition, links may be provided from this website to other websites which are not owned or controlled by Arusha Municipal Council. Please be aware that the Arusha Municipal Council is not responsible for privacy practices of such other website and that when such link are selected, user shall be leaving AMC website and be bound by privacy policy of those websites.

17 EMAIL DISCLAIMER

This e-mail message shall not be construed as legally binding on the Arusha Municipal Council (AMC). As internet communications are not secure, AMC does not accept responsibility for the content of this message.

This message is intended only for the recipient(s) named above. Any unauthorized disclosure, use or dissemination, either in whole or in part, of this message is prohibited. If you have received this message in error, please inform the sender immediately by return e-mail and delete this message and any attachments thereto from your system.

Thank you for your cooperation.

ICT PROCUREMENT FORM

ICT UNIT
Asset issued & Hand over voucher

1. USER INFORMATION

First, Last Name: ……
Title: ……..
Department: …….
Section: ……..
Unit: ……..

Date: ……..
ID #: ……..
Ext #: …….
Room #: ……
Signature: ……

2. ISSUED EQUIPMENT

Barcode Number	Serial Number	BT Number	Description

3. RETURNED EQUIPEMENT

BT Number	Serial Number	Description

……. ……..
Signature of ICT staff carrying out The Physical Verification

Name of ICT staff verifying ICT Equipment

……. ……

Date posted to Inventory

Name if ICT staff posted by

ICT SERVICE REQUEST FORM

ARUSHA MUNICIPAL COUNCIL
P.O.Box 3013 Arusha,Tanzania
Tel: 2508073 / 2503494 **Fax:** 2505013

ICT UNIT

Service Request

Requested by: ……
Extension: ……
Designation: ……..
Section: ……
Name of ICT -Tech: ……

Time: ……
Date: ……
Request taken by: ……
Forwarded: ……..
Time Tech: Received: ……

Type of Request
Check the relevant option

( ) Application
( ) Hardware
( ) Others
( ) Networking
( ) Platform (OS)
( ) Software

Description
Please give a full description below for each of the above selected options,

……
……
……
……
……

User's comments……....
Signature…….

For Internal ICT Unit Use only

Approved By: ……. Signature: ……

☐ Completed Pending Referred to: …….

Completed By	Date	Time	Comments