THE UNITED REPUBLIC OF TANZANIA

PRIME MINISTER'S OFFICE REGION ADMINISTRATION AND LOCAL GOVERNMENT

SENGEREMA DISTRICT COUNCIL

INFORMATION AND COMMUNICATION TECHNOLOGY(ICT) POLICY

District Executive Director
P.O.Box 175
SENGEREMA
TEL: 028 2590162
FAX: 028 2590249
E-MAIL: dedsengerema@ymail.com

July 2014

EXECUTIVE SUMMARY

This document describes an Information and Communication Technology(ICT)Policy for the Sengerema District Council (SDC). The policy lays down general guidelines and framework for the use and management of the Council's ICT resources/infrastructures.

In formulation of this policy,the District Council has drawn experince from the National ICT policy and other Comparable organizations and has made references to the international best practices in Information Technology(IT).Views from the Council's employees have also been accommodated.

The primary objective of this policy is to ensure that all ICT resources and systems of the Council 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 Equipments 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 Council's ICT resources

The council will endeavour to ensure that the users of the Council's ICT resources are kept abreast of new development and advancement in ICT,the risks that the Council's ICT resources continue to be exposed to ,and the available risk mitigation initiatives that need to be applied.The Council 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 council.

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

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

TABLE OF CONNTENTS

EXECUTIVE SUMMARY 1
TABLE OF CONNTENTS iii
GLOSSARY v
LIST OF ACRONYMS ix
1.0 Background 1
2.0 Policy Objectives ,Roles and Responsibilities 2
2.1 Objectives 2
2.2 Roles and Responsibilities 2
2.3 ICT Organization Structure 3
2.3.1 ICT Committee 3
2.3.2 Head of ICT Unit (System Analyst) 3
2.3.3 System Administrator 4
2.3.4 Network Administrator 4
2.3.5 Database Admistrator 4
2.3.6 Webmaster 5
2.3.7 Computer Technician(Computer Operator) 5
2.3.8 Public Relation Officer 5
2.4 Head of Internal Audit Unit 6
2.5 Users of IT sytems 6
2.6 Compliance and Penalties 6
2.7 Management of ICT resouces. 6
2.8 Asset Tracking/Inventory 6
3.0 ACCEPTABLE USE AND OWNERSHIP OF DATA 7
3.1 Acceptable Use 7
3.3 Ownership of Data and Information. 8
4.0 PROCUREMENT OF IT EQUIPMENT AND DISTRIBUTION 8
4.1 Planning Acquisition 8
4.2 ICT Resources entitlement 8
4.3 Procurement of ICT Resources 9
4.4 Lifetime and Replacement of ICT Resources 9
5.0 INFORMATION SYSTEM USE 9
5.1 Systems Access 9
5.2 User ID and Password 10
5.3 Use of the Available System 10
6.0 INFORMATION SECURITY 10
6.1 Information Protection 11
6.2 Protection against Hazards 11
6.3 Physical Access to Servers and Server room. 11
6.4 Data Backup 12
6.5 Data Restoration 12
6.6 Antivirus Measures. 12
6.7 Third Party System Support. 13
6.8 Repairs of Computers 13
6.9 Audit Trail 13
7.0 WEB-BASED APPLICATION 13
7.1 Access and Use 13
8.0 WEBSITE 14
8.1 **Website Management** 14
9.0 COMMUNICATION POLICY 14
9.1 Intranet 14

9.2 Internet Browsing.....14
9.3 Email.....15
10.0 RESOURCES MANAGEMENT.....15
10.1 Hardware.....15
10.2 Business Resumption.....18
11.0 ICT GUIDELINES.....18
12.0 MONITORING AND EVALUATION.....18
13.0 POLICY REVIEW.....19
APPENDICES.....20
AUTHORISATION AND APPROVAL.....24

GLOSSARY

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

Word(s)	Meaning
Access Controls:	Meaning of establishing and enforcing rights and privileges allowed for users
Access Rights:	Authorized entry into a computer system to read,write,modify,delete or retrive 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 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.
Compliance:	To act according to certain accepted standards or rules.
Computer Networks:	A collection of computers and devices Interconnected in order to enable resources sharing.
Confidentiality:	The protection of information from unauthorized disclosure.
Data	Basic facts and figures that can be processed to useful information.
Database Administration:	The role generally associated with the management and control of a Database.
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.

Word(s)	Meaning
Database:	A collection of data that is organized so that its contents can easily be accessed managed and updated to serve multiple users.
Division:	Means a directorate/unit as described in SDC's Organizational structure.
E-mail System:	All means of sending,receiving and storing electronic mails(e-mails)
Employee:	A person employed by the District Director on Permanent or contractual terms.
Encryption:	A conversion of messages(data/voice/video) into a form that can not be understood by unathorized readers.
End Users:	All Users of IT systems including system Developers and Administrators
Full Council:	The District Councilor's general Meeting
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 Resouces:	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 unathorized access,use,disclosure,disruption,modification,or destruction.
Information System:	The term that encompasses all components required for the processing of information eg.Application,Databases,Operating Systems and Network components.

Word(s)	Meaning
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 Council.
Integrity:	The protection of information/data from authorized,unanticipated or unintentional modification or deletion,or to be able to identify such action when it can not 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 District's Management Team consisting of heads of divisions
Mass Storage:	Device that can store large amounts of information.
Mass-mail:	E-mail 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 device that facilitates 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.

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 powerfull 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 licencing 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 Council's Staff Regulations.
Standards:	Specified uniform use of tools,techniques and methods to implement policy or procedure.
System Administration:	The role associated with the management and controll 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 Council,including consultants,contractors,vendors,agents,and personnel affiliated to them.

Word(s)	Meaning
Users:	Include Council's employees,temporary workers,external contractors,consultants,external auditors or any othe parties which entered into an agreement to provide a service to the Council and obtain access to Council's information system and use Council's systems.
Virus:	A Computer program that can copy itself and infect a computer withou 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 Service 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
SDC	Sengerema District Council
VPN	Virtual Private Network.

1.0 Background

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

The Policy applies to all Sengerema District 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 Sengerema District Council.

The purpose of this policy is to set both policies and guidelines for use Sengerema District Council Computers and access to Files,E-mail and internet systems by the user of the system.

There are various reason for the need of a policy/guideline, for instance:
A good policy protects both the employer and emploee from misuse of Files,Applications,the Internet,E-mail and other electronic interfaces that might develop in the future.With the rapid evolvement of the internet and related system there has been

Enough scope for misuse to grow and build-up withou adequate procedures being put in place to regulate acceptable behaviour.

In putting into place a policy, Sengerema District 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 Sengerema District Council to protect itself and the employees from misuse of Sengerema District 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 consequences that such action by a user might lead to,should be unambiguous to all concerned.

The aim of the policy is not to be restritive,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 Sengerema District Council and the user should not be detrimental.

2.0 Policy Objectives ,Roles and Responsibilities

This Policy lays down general guidelines and framework for the use and management of the Council's ICT resources.It spells out the do's and dont's in the use of the Council'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 Technology resources and systems of the District 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 Full Council,District Executive Director,ICT Commitee,Management,Head of ICT unit and other users of ICT systems of the District.

2.2.1 The Full Council

The Full Council 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.

2.2.2 District Executive Director

The District Executive Director shall:

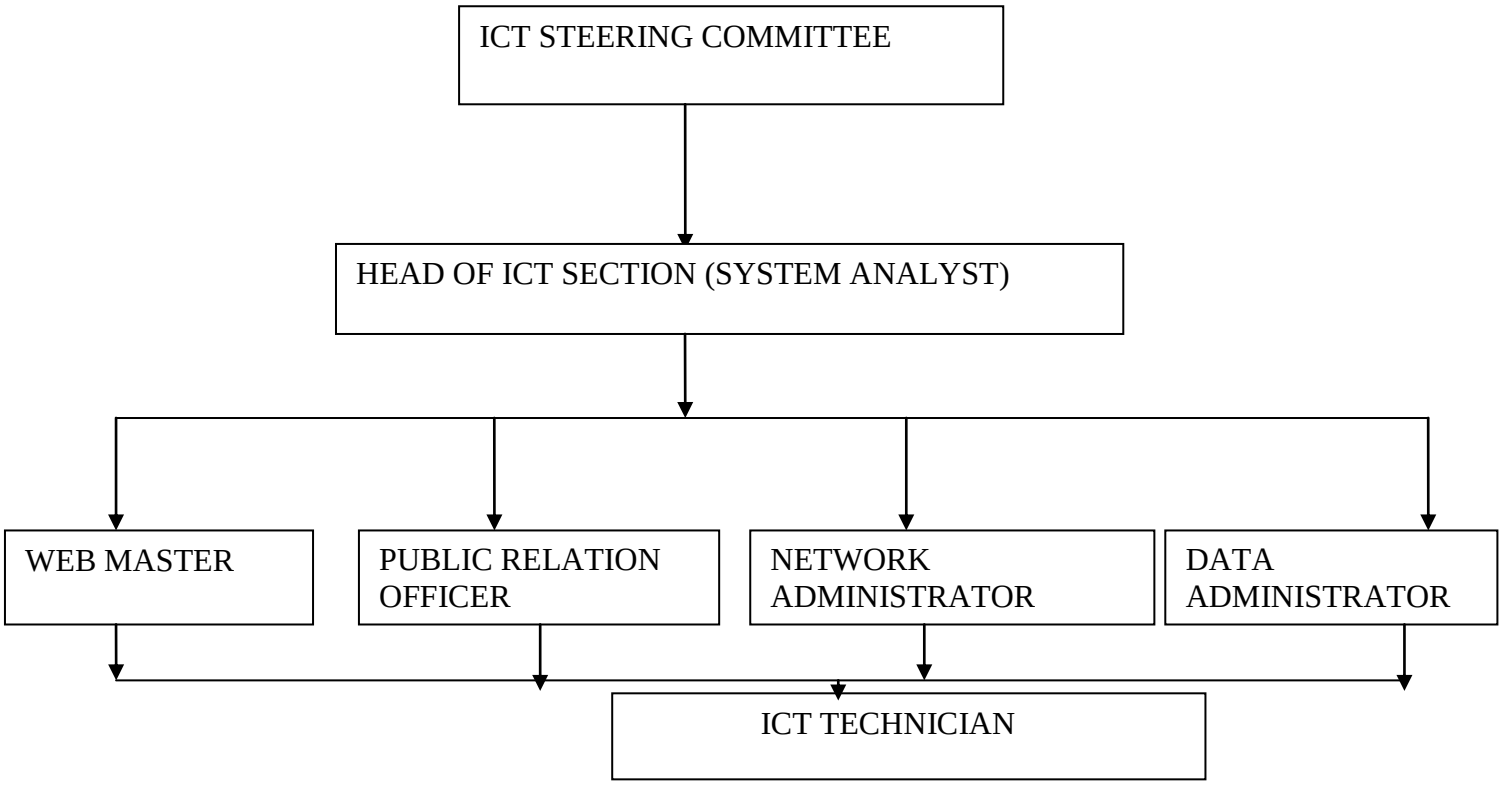
i. In consultation with the head of ICT unit (System Analyst) appoint a commitee (hereinafter referred to as "ICT Committee") and determine its term of reference.
ii. Recommend to the Full Council an appropriate ICT Policy for the District; and
iii. Ensure the implementation of the policy.

2.2.3 Council Management Team(CMT)

Council Management Team shall:-

i. Ensure that all users under their supervision are aware and comply with the Policy:
ii. Provide adequate and appropriate protection to ICT assets and resources under their control;
iii. Ensure availability,integrity and confidentality of information produced by system under their areas of functional responsiblities,and thereby ensure continuity of operations:and
iv. Review and approve procedures,standards,rules and guidelines developed from this Policy for the purposes of maintaining business continuity and security of the District's ICT resources.

2.3 ICT Organization Structure



2.3.1 ICT Committee

Responsibilities of the Commitee shall include to:

i. Propose SDC's ICT Policy for approval by management.
ii. Coordinate the establishment and continued review of SDC ICT policy and strategy.
iii. Ensure that all the ICT strategy is aligned with the SDC's Plans;
iv. Advice the District Executive Director in making considered decisions about the focus of the ICT resources;
v. Review all ICT services and Applications including District website and infrastructure,with the view to advice the District on required improvements;and
vi. Ensure that the risks associated with ICT are managed properly.

2.3.2 Head of ICT Unit (System Analyst)

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

i. Coordinate the review and amendment of the Policy, as when required in order

to accomodate new technologies or servises, applications, procedures, perceived dangers;

ii. Plan and develop ICT security strategies;
iii. Monitor adherence to the ICT Policy and 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 District's sytems in particular;
v. Initiate and recommends proposals to change,modify or improve the Policy.
vi. Recommend Procedures,standards and rules for ICT function and effective implementation of the policy.
vii. Overall incharge of the ICT function.

2.3.3 System Administrator

The System Adminstrator shall;

i. Provides administrative and technical guidance to the users of information sytems at the District.
ii. Performs routine monitoring of servers.
iii. Provide help desk services to sytem users.
iv. Provides sytems user id with different access level rights.
v. Perform Periodic backup and disaster recovery.

2.3.4 Network Administrator

The network administrator shall

i. Monitor network communication
ii. Update system as soon as new version of OS and application software comes out
iii. Implement the policies for the use of the computer system and network
iv. Setup security policies for users.
v. Maintain and administer computer networks and related computing environments, including computer hardware, systems software, applications software, and all configurations.
vi. Plan, coordinate, and implement network security measures in order to protect data, software, and hardware.
vii. Operate master consoles in order to monitor the performance of computer systems and networks, and to coordinate computer network access and use.
viii. Perform routine network startup and shutdown procedures, and maintain control records.

2.3.5 Database Admistrator

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

2.3.6 Webmaster

i. Develop and continually update the District's website

2.3.7 Computer Technician(Computer Operator)

i. Helps install local area network cabling systems and equipment such as network interface cards, hubs and switches.
ii. Identifies, diagnoses, and resolves Level One problems for users of the Server, personal computer software and hardware, Council network, the Internet and new computer technology in a call center environment; communicates solutions to end-users.
iii. Perform regular backup system for in-office desktop computers and file servers for SDC.
iv. Provides one-on-one end-user problem resolution over the phone or direct (Physical contact) for District approved Personal Computer (PC) software.
v. Delivers, tags, sets up, and assists in the configuration of end-user PC desktop hardware, software and peripherals.
vi. Performs minor desktop hardware repair for PC computer equipment and peripherals that are not diagnoses and resolves end-user network or local printer problems, PC hardware problems and mainframe, e-mail, Internet, dial-in and local-area network access problems.
vii. Perform all other duties which will be assigned by Computer System Analyst.
viii. Installing, Updating, and troubleshooting computer Operating system and application program.

2.3.8 Public Relation Officer

i. Planning, developing and implementing PR strategies;
ii. Liaising with colleagues and key spokespeople;
iii. Liaising with and answering enquiries from media, individuals and other organisations, often via telephone and email;
iv. Researching, writing and distributing press releases to targeted media;
v. Colleting and analysing media coverage;
vi. Writing and editing in-house magazines, case studies, speeches, articles and annual reports;
vii. Preparing and supervising the production of publicity brochures, handouts, direct mail leaflets, promotional videos, photographs, films and multimedia programmes;
viii. Devising and coordinating photo opportunities;
ix. Organising events including press conferences, exhibitions, open days and press tours;
x. Sourcing and managing speaking and sponsorship opportunities;
xi. Commissioning market research;
xii. Fostering community relations through events such as open days and through involvement in community initiatives;
xiii. Managing the PR aspect of a potential crisis situation.

2.4 Head of Internal Audit Unit

The head of Internal Audit Unit of the Council shall audit the IT Unit and ensure compliance with the ICT policy of the Council.

2.5 Users of IT sytems

The head of Internal Audit shall audit the IT unit of the District council against all types of threats and alert management of all vulnerable areas. The users shall also comply with alert management of all vurnerable areas,Users shall also comply with all security controls set out in this policy and other regulations of the District.

This policy, entirely shall be made available to all employees of the District who shall make themselves familiar with the relevant section and sign a user acceptance Form.

2.6 Compliance and Penalties

i. All Employees and other authorized User's of the District's ICT resources shall comply with the requirement of this policy.
ii. The head responsible for IT shall enforce compliance by using audit trails on all IT resources used at the District.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 Policy can lead to withdrawal and/or suspension of system and network privileges and/or other disciplinary action to be determined by Management.

2.7 Management of ICT resouces.

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

2.8 Asset Tracking/Inventory

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

3.0 ACCEPTABLE USE AND OWNERSHIP OF DATA

3.1 Acceptable Use

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

i. All networking and computing systems and resources which include but not limited to the Internet,Intranet,printing,software,storage media and network accounts for electronic mail or other access permission,are the property of the District.
ii. IT resources are to be used for the purposes of advancing the District's mandate.Inappropriate use of IT resources may expose the District to risks including but not limited to loss of these resources,virus attacks and legal implications.

3.2 Physical and Sytems Access.

i. Networking and Computing equipment entrusted to Users must be secured against any threats.
ii. The District's server(s) room shall be kept in a secure server room.
iii. All entries to the server room must be recorded and security camera be installed to monitor all accesses.
iv. Desktop Computers,laptop,scanners,printers and other peripheral equipment or systems under User's custody must be handled with proper care to avoid damage,dusts etc.
v. Computer application must be closed and users must log off from the system when the system is not in use.
vi. All equipment must be switched off properly before Users leaves the Office.
vii. Power protections on equipment must not be by-passed withou proper authorization by Head of IT Unit.
viii. Users are not allowed to install hardware and personal software,including device drivers or change configurations on the District's networkin or computing systems.
ix. Users shall no allow non –SDC individuals to use IT resources assigned to them without prior written authorization.
x. All movement of IT equipment must be authorized by Heads of Departments through a written form and the movement supervised by the Head of IT Unit.
xi. All computing and networking installations must be protected and made secure by the District's IT Unit.Problems related to installations or malfunctions must be reported to the IT Unit.
xii. 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 District's computer facilities shall remain the property of the District.
ii. Any Department,Section or Unit within the District 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 withou authorization from the District Director.
iv. All software created by the District shall be exclusive propery of the District, and shall not be transferred,given or distributed to any organization or individual without the written authorization of the District.
v. All software Licenced to the District shall not be transferred,given or distributed to any organization or individual.

4.0 PROCUREMENT OF IT EQUIPMENT AND DISTRIBUTION

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

Procedures for planning,procurement,distribution,utilization and disposal of ICT resources for the District are outlined here under.

4.1 Planning Acquisition

i. All user departments shall establish and submit,in writting ,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 IT Unit for procurement on the need-basis.

4.2 ICT Resources entitlement

i. ICT resources will be allocated as per the District 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 ICT Resources

i. Specifications for procurement of ICT resouces 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 resorces 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 the District's financial regualtions.
iii. In disposal of obsolete ICT resources described under(ii) above,priority disposition shall be given to employee(s) who was allocated the ICT equipment under disposal.

5.0 INFORMATION SYSTEM USE

This Section streamlines the use of information stored into differenet 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 password,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 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 through the specified form.
iv. Access to any system shall always be through the provided application software 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 District ownership shall not be used unless authorized by the IT 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,spouce) years of birth,or login name.

ii. Passwords for IT resources must be discrete and alphanumeric,both upper and lowercase 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 IT administrators and should not be written down or stored on-line

v. Initial passwors 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 IT system once the system has been approved.

ii. Heads of Department shall demand specific reports from sytems 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 IT 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.

6.0 INFORMATION SECURITY

This Section is set to ensure that the District'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 District's Information assets are protected against theft,disclosure,leakage,piracy and destruction.
ii. Users shall not disclose their password.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.
v. Users shall not disseminate any of the District's information or data to unauthorized persons or organization without the authorization of the District Director.
vi. Users shall ensure that any discarede information or data is properly collected,stored and destroyed according to the procedures and guidelines on information destruction
vii. Users shal,regularly update their antivirus and the IT Unit shall ensure that computers are installed with up to date versions of antivirus.
viii. Users shall ensure that all computers or information storage to be discarde,disposed of,or sent outiside the District;s premises for any purpose,have all the information or data removerd from them.
ix. Users shall keep and store all the District data and Information into the respective folder in the assigned network drives on the servers,which will be backed regularly.

6.2 Protection against Hazards

i. Power supply to the IT equipment must be checked to ensure that it is available and safe for the equipment.
ii. Management must ensure that all IT resources are protected against natural hazards including fire,floods and lighting.
iii. Server rooms must 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 standadrs.
ii. Server rooms must not be accessible to unathorized persons.
iii. Access to servers must bear prior written approval from the head of IT Unit.
iv. All administrator to Servers computers.
v. Shall be done remotely from computers other than the server themselves unless it is extremely necessary
vi. Server rooms must have special measures against theft.

6.4 Data Backup

i. Sytems and data backup must be perfomed 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 on two separeate media and stored in phisically separate locations to be specified by thr IT UNIT
iii. Users shall be assisted by the IT unit to backup their individual inforamtion in their respective at leat one a year.
iv. The IT unit must ensure that all strategic systems are stored in the Server and are backed regularly.
v. Management must provide resoucers 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 IT Unit must ensure that restoration procedures are tested using valid backups.

6.6 Antivirus Measures.

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

6.7 Third Party System Support.

i. IT 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 District's network system.
iii. Third Party system support may be allowed to use their IT tools for their work whenever it is necessary.However their computers must be scanned for viruses before they are connected into the District's computer network.
iv. Third Parties Systems Support is prohibited from copying any information or data from District'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 IT Unit.

6.8 Repairs of Computers

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

7.0 WEB-BASED APPLICATION

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

7.1 Access and Use

i. The District through the IT Unit shall grant relevant access rights and privileges to third parties.
ii. Third parties access to the District's web-based application will be through a VPN Clients.
iii. Users shall always log off and close the web-bases application when not using the system.
iv. Wrongly posted to the District's web-based applications by third parties shall immediately be reported to the District.
v. Users ID and Passwords must not be shared availed or made known to others.

vi. Any abnormalities,erros or loopholes in the system must be reported to the District IT unit.

8.0 WEBSITE

This Section establishes guidelines on handling the contents of the District's website and how and when the information shuold be updated.

8.1 **Website Management.**

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

9.0 COMMUNICATION POLICY

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

9.1 Intranet

i. IT Unit shall be responsible for publishing and updating Information on the Intranet
ii. All official communication within the District 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 District reserves the right to monitoer 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 District 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 Users.

iii. All browsing on the Internet should ensure District's interest is higher than users.
iv. Browsing of Pornographic sites is prohibited.
v. Users are not allowed to install software downloaded from the 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 District'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 District'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 larger 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 District Director.
vii. Official Email addressed to organizations or individulas outside the Council must clearly identify the user by full name,position and contact address in the District.
viii. E-mails shall bear standard disclaimer.
ix. The District reserves the right to inspect,monitor and disclose the contents of any email created,sent,received or forwarded by using the District computer networks or email sytem.
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 District mail account at least two(2)times per day to ensure timely handling of Information.

10.0 RESOURCES MANAGEMENT

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

10.1 Hardware

All hardware devices acquired for or on behalf of District or developed by District employees or contract personnel on behalf of District is and shall be deemed District property.All such

hardware devices must be used in compliance with applicable licenses,notices,contracts and agreements.
The following standards will be used for District IT equipments(excluding test computers)that are fully supported by the IT Unit.

10.1.1 Servers Standards

i. Servers will be installed and mainted in the designated Server room that meet proven standards.
ii. Servers will be based on the 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 moutable 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 specification shall be reviewed each year and speciafied according to requirements but shall be below 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 office.
ii. Laptop will be provided to employess 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 District minimum specification requirement.
v. All desktops computers shall be powered by UPS and laptop protected by electric surge protector.
vi. Laptops will be provide to employee with appropriate security locks.

10.1.3 Monitors

i. Monitors will be provide 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 IT Unit.
iii. Employees needing computer hardware other than what is stated above must request such as hardware from the IT Unit.Each request will be considered on a case by – case basis in conjuction with the Public procument regulations.

10.1.5 Hardware from Outside.

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

10.1.6 Hardware to Outside.

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 from this regard.

10.1.7 Software

i. All software procured by the District or developed internally shall be the property of District.
ii. All software must be used in comliance with applicable licences,notices,contracts,agreements.

10.1.8 Licensing

i. All software by the District shall be properly licensed.Unless otherwise provided in the applicable licence,notice ,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 standars

The following list shows the standards suite of software installed on the District computers(excluding test computers) that is fully supported by the Head of IT Unit.

10.1.9.1 PC's Environment

The PC's environment shall consist of the following:

i. Microsoft XP Professional/Vista/7(As current standard client operating sytems)
ii. Microsoft Windows compatible messaging utility(ms Outlook and Ms Outlook express)
iii. Office productivity applications ashall 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 2008 or above
ii. Red Hat Linux Version (
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 the District's operation requirements.Departmant that require software other than
Those prescribed above should request the same from IT Unit.

10.2 Business Resumption

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

11.0 ICT GUIDELINES

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

i. Maintainance and Outsorcing;
ii. Disk and Data Sanitation; and
iii. Risk Mitigation.

The detailed guidelines are attached.(Appendix 5)

12.0 MONITORING AND EVALUATION

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

i. Automated auding/monitoring mechanisms.
ii. Physical Inspections;and
iii. Internal Auditing findings.

13.0 POLICY REVIEW

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

APPENDICES

a) DECLARATION BY USERS

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

(Declaration By District Employee)

I, _____ (Full name)

Acknowledge that the District'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 District shall take against me appropriate disciplinary action or legal action,or both,as the case may be.

Signature: : _____.

Department: _____.

Job Title: _____.

Date: _____/_____/_____.

b) DECLARATION BY THIRD PARTY

I, _____ of

_____,

(name of your company and full address) do hereby acknowledge that the District 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 employement 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: : _____.

Department: _____.

Job Title: _____.

Date: _____/_____/_____.

c) 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 Sengerema District 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 Sengerema District Council be liable for any damage arising,directly or indirectly,from use of the information contained in this website including damages arising from inaccuracies,omissions 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 Sengerema District Council hereby disclaims any liability and shall no be held liable for any 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 Sengerema District Council.Please be aware that the Sengerema District Council is not responsible for privacy practises of such other websites and that when such link are selected,user shall be leaving SDC website and be bound by privacy policy of those websites.

d) EMAIL DISCLAIMER

This e-mail message shall not be construed as legally binding on the Sengerema District Council(SDC).As internet communications are not secure,SDC 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 attachment thereto from user system.

Thank you for your cooperation

ICT SERVICE REQUEST FORM

ICT PROCUREMENT FORM

ICT UNIT

Assets issued & Hand over Voucher

1. USER INFORMATION

First,Last Name:..... **Date:.....**
Title:..... **ID#:.....**
Department:..... **Ext#:.....**
Section:..... **Room #:.....**
Unit:..... **Signature:.....**

2. ISSUED EQUIPMENT

Barcode	Serial Number	BT Number	Descriptions

3. RETURNED EQUIPMENT

BT Number	Serial Number	Descriptions

....
Signature of ICT staff carrying out The Physical verification
Name of ICT staff veryifing ICT equipement

....
Date posted to FACS
Name of ICT staff posted by

SENGEREMA DISTRICT COUNCIL

SENGEREMA DISTRICT COUNCIL
P.O Box 175 Sengerema,Mwanza
Tel:028-2590162 Fax: 028-2590249

ICT UNIT

Service Request

Requested by:	Time:
Extension:	Date:
Designation:	Request taken by:
Section:	Forwarded:
Name of ICT-Tech:	Time Tech :Received:

Type of Request
Check the relevant option

Application	Networking
Hardware	Platform (OS)
Others	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:.....

AUTHORISATION AND APPROVAL

Authorised By		*Approved By*	
Name		**Name**	**Hon Methew Lubongeja**
Signature		**Signature**	
Designation	District Executive Director	**Designation**	Council Chairman
Date		**Date**	