INFORMATION AND COMUNICATION TECHNOLOGY (ICT) AND RISK MANAGEMENT POLICY FOR KAZO DISTRICT LOCAL GOVERNMENT.

FOR GOD AND MY COUNTRY

THE REPUBLIC OF UGANDA

KAZO DISTRICT LOCAL GOVERNEMENT

Prepared by:

AGABA NELSON

IT OFFICER

AUGUST 2021

ICT POLICY AND PROCEDURES

1. Acceptable and Un acceptable Use of ICT Resources
2. Internet usage
3. ICT Security
4. Management Information Systems
5. Procurement and Disposal of ICT equipment
6. Maintenance and Repair

LIST OF ABBREVIATIONS

CAO	Chief Administrative Officer
DRP	Disaster Recovery Plan
ICT	Information and Communication Technology
LAN	Local Area Network
LG	Local Government
M&E	Monitoring and Evaluation
MIS	Management Information System
MDA	Ministry, Department and Agency
PDU	Procurement and Disposal Unit
PPDA	Public Procurement and Disposal of Assets
PWDS	Persons with Disabilities
SLA	Service Level Agreement
PC	Personal Computer
IT	Information Technology
LLG	Lower Local Government
IPPS	Integrated Public Payroll System
IFMS	Integrated Financial Management Systems
PBS	Program Budgeting System
KDLG	Kazo District Local Government
LAN	Local Area Network
WAN	Wide Area Network
VPN	Virtual Private Network
ISP	Internet Service Provider
NITA-U	National Information Technology Authority Uganda

FOREWORD

The Purpose of this Policy is to describe and document the ICT Policies and procedures that will support the district's goals and objectives. This geared towards increasing effectiveness and efficiency in all the district administration functions.

This policy is aligned to existing District and National Policies, Strategies and laws as well as globally recognized ICT best practices.

The District Administration will accordingly ensure that this policy is disseminated to all the LG administration staff and that it is effectively adhered to.

This policy will be periodically reviewed after every three years to ensure that the policies set are up to date and aligned to the goals of the district.

Signed

KAZO DISTRICT LOCAL GOVERNMENT
10 JAN 2022
DISTRICT CHAIRPERSON

REV. SAMUEL MUGISHA KATUGUNDA
DISTRICT CHAIRPERSON
KAZO DISTRICT LOCAL GOVERNMENT

ACKNOWLEDGEMENT

Today Information Technology is one of the drivers of development. Without information and communication, you are kept outside the globe. Starting from a phone, you are communicating and making business from home.

Kazo District Local Government is desirous to use the Information Communication Technology to spur development of the district through quick service delivery to the community.

So the delivery of service through Information Communication Technology has to be used in a principled manner in order to spur this development. However, technological advancements like the Internet have digitally broken the geographical, physical, political and even sociological divide, transforming the world into a Global Village. As a result, cyber-crime is progressively increasing. This calls for regulated and guided interventions to address the ICT related issues.

To this end, I thank the district technical staff and the District Council for providing funds to come up with this policy. I hope once this policy is implemented with the utmost guidance it requires, the District will deliver services to her people in the most effective and efficient manner.

NSUBUGA ZIRIMENYA
CHIEF ADMINISTRATIVE OFFICER
KAZO DISTRICT LOCAL GOVERNMENT

CHIEF ADMINISTRATIVE OFFICER
10 JAN 2022
KAZO DISTRICT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The utilization of Information and communication Technology (ICT) is on the rise in both public and private sector to embrace E-Governance. Kazo District Local Government has embraced E-governance in order to meet its mission, goals and objectives in a more effective manner by speeding up service delivery processes. The purpose of this policy is to establish acceptable and unacceptable use of ICT Equipments and network resources with its established culture of ethical and lawful behavior, openness, trust and integrity in order to maintain the confidentiality, integrity and availability of its information assets. This policy requires users of information assets to comply with organization policies. Kazo District ICT policies include Acceptable and un acceptable use of ICT resources policy, Internet usage policy, ICT security policy, Management Information Systems Policy, Procurement and Disposal of ICT equipment policy, Maintenance and repair policy.

1.0 INTRODUCTION

1.1 Policy Overview

1.1.0 Rationale for the ICT policy

Recent technological advancements like the Internet have digitally broken the geographical, physical, political and even sociological divide, transforming the world into a "Global Village". As a result, cyber-crime is progressively increasing. This calls for regulated and guided interventions to address the ICT related issues.

The utilization of IT (Hardware, Software and E-Applications) is on the rise in both public and the private sector. There is need for proper laws and guidelines to be developed to guide its utilization.

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network recourses at Kazo District Local Government in conjunction with its established culture of ethical and lawful behavior, openness, trust and integrity.

Kazo District Local Government provides computer Devices, Networks, and other electronic information systems to meet missions, goals, and initiates and must manage them responsibly to maintain the confidentiality, integrity and availability of its information assets. This policy requires the users of information assets to comply with organization policies and protects the organization against damaging legal issues.

1.2 Policy Philosophy

Through Information Technology the District aims to prepare staff to participate in a rapidly changing world. Increased ICT skills promote independent learning and give greater access to a wide range of ideas and experiences. It enhances the quality of staff's work across their operations and should enhance and enrich the service delivery process in the district. All staff from support staff to Officers have access to information and communications technology.

1.3 Vision

Having a prosperous population readily accessing quality ICT Services

1.3 Objectives

1.3.1 Main Objectives

Provision of quality ICT services for effective

1.3.2 Policy Goal

To guide the optimal development and utilization of ICT in the district

1.3.3 Policy Objectives

The staffs are encouraged to develop confidence in using hardware and software and other IT equipments.

To use ICT to manipulate and present written work, images and sounds to convey information effectively.

To promote widespread use of IT applications in both public and private sectors to enhance efficiency and effectiveness in service delivery within the district.

To store information, retrieve it and present it in ways which enhances interpretation and analysis.

To be aware of the role of ICT in the control of equipment encountered in daily life.

To be able to discuss the use of ICT and its place within real contexts.

Through providing appropriate experiences, staff will achieve ICT competence, acquiring knowledge about the application and implications of ICT, the necessary skills to apply ICT in a variety of contexts and a better understanding of the role and potential of ICT

To sensitize communities about IT services as well as promotion and awareness campaigns in the communities.

1.7 Policy scope

All employees, intern students, contractors, consultants, temporary and other workers at Kazo District Local Government, must adhere to the policy. The policy applies to information assets owned or leased by Kazo District Local Government, or to devices that connects to the District Council network or reside at Kazo District Local Government website.

ICT Committee must approve exceptions to this policy in advance through getting approval from ICT Officer.

Legal framework

The district ICT policy shall be in line with the following laws and policies:

1. The constitution of the republic of Uganda (1995)

2. The national ICT policy (2013)
3. The communications Act (2013)
4. The phonographic act (2014)
5. The computer misuse act (2011)
6. The electronic transactions act (2011)
7. The access to information act (2005)
8. The Uganda human rights act, Cap.24s
9. The national information technology authority Act, 2009
10. The Uganda communication Regulatory authority Act, 2012

1) **Policy Guiding principles**

4.1 Mainstreamed and integrated ICT services

This policy will assist in mainstreaming and integrating ICT services in the district administration business processes. This will be in areas such as automating, transforming and providing accurate, timely and quality information for decision making

4.2 Protected ICT Asset and Equipment

The development of this necessitated by the need for both physical and digital protection of ICT assets and equipment to ensure safely of all the district ICT resources

4.3 Secure and Reliable ICT Environment

The need for this policy is backed by the need to provide secure and reliable environment in which to run the ICT services. To build confidence among users and to enable business re-engineering process for effective and efficient service delivery is a cornerstone of this policy.

Continuous Systems and Business Process Improvements

This policy helps in identifying, understanding and managing a system of interrelated business processes to keep the district administration up to date and in tandem with the ever-changing ICT environment.

4.5 Accessibility and ease of use of ICT services

This policy sets a framework for accessible and easy to use ICT services. Thus providing an important opportunity for improving the productivity of both staff and external stakeholders that access the district ICT systems.

4.6 Focus on persons with Special Needs

While talking cognizance of fundamental human rights, this policy sets a background for providing ICT services and infrastructure that are responsive to the needs of persons with Disabilities (PWDS). This will enhance the ability of PWDS to obtain services from the district administration and also to serve as district staff.

4.7 Training and Technical Support

This policy sets a frame work for ensuring that there is sustained training and that appropriate technical support is provided to the district staff/users.

4.8 Adaption of best practices and ethics

The policy ensures that all users of the district ICT resources adhere to best practices as they ethically execute their duties.

Scope of the policy

The ICT policy applies to local the district local government administration departments and units. The policy covers the following specific areas:

1. ICT service Management
2. Date Communication
3. Information Security
4. Software Development and Acquisition
5. ICT Skills Capacity Development
6. ICT Services Support
7. Telecommunication and Unified communications
8. ICT Procurement
9. Social Media
10. Software Licensing and Ownership

11. Information System and Data warehousing
12. Special Needs ICT Usage

ICT Services Management

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

6.1 Roles of the Staff

The ICT Steering Committee shall have its representation as determined by the District Technical Planning Committee. Officers within the TPC shall advise and act as members on the ICT committee. The committee shall:

1. Advise and monitor the implementation of ICTs in the District;
2. Ensure provision of resources within the District Budgeting process for implementation of ICTs;
3. Ring fence 2% of the Districts total budget for Locally raised revenue expenditure on ICTs;
4. Inclusion of ICT support within all the Districts Grants in tandem with respective grant guidelines;
5. Monitor development and innovations in the ICT sector, in order to advise on implementation of innovative and sustainable ICT solutions aligned to District's strategic goals
6. Undertake advocacy for the adoption and utilization of ICTs within the District Administration and
7. Act as champion Agents in the enforcement of the ICT policy.

6.1.2 ICT Office

The Department of Administration shall be the mother department for the ICT Support Function at the District. An ICT Office shall be set up with relevant and qualified personnel. The duties of the ICT office shall include

1. Provision of effective ICT Support that is responsive to the functions and business need of the District Administration;
2. Promoting effective and appropriate utilization of ICT resources;

3. Identifying and communicating to the District Administration any emerging needs;
4. Providing a forum for the continuous evaluation and assessment of existing ICT services and infrastructure;
5. Promoting an environmentally friendly approach to the acquisition, use and disposal of ICT resources;
6. Coordinating resource mobilization for counterpart funding for the implementation of ICT policy and strategy;
7. Specifying, verifying and vetting ICT standards, procedures and best practices for all District ICT deployments and operations;
8. Having the overall ownership of the professional and technical mandate of all ICT design and developments, management and maintenance;
9. Liaising with ICT Service providers;
10. Operationalizing the ICT policy.

6.1.3 Heads of Departments/Units

The Heads of Departments and Units shall in consultation with the ICT Office carrying out the following;

1. Integrate ICTs activities into their activities;
2. Implement the department –specific components of the District ICT policy and strategy
3. Ensure compliance to the District ICT policy and
4. Actively participate in supporting and facilitating the effective implementation of the ICT policy and strategy.

6.1.4 District Staff;

The district Staff shall ensure compliance to the ICT Policy as they execute their duties.

The ICT Office has the responsibility for support and problem resolution for software and hardware. To effectively carry out that role, the ICT Office must be able to rely on standard hardware and software configurations. Users must request hardware and software through the ICT sector.

6.2 Hardware Standards

The current hardware for use at District is with the ICT Office. Unit heads who have a need to deviate from the standards must request an exception. The CAO will review the request and either approve request as is, or suggest alternate solution to ensure support can be provided.

6.3 Software Standards

The ICT Office must first acquire and test programs, before it is utilized on the District's ICT equipment. Software may only be used in compliance with the terms of the applicable licenses agreements.

6.4 Unauthorized Software

Use of unauthorized software can degrade the District's computing resources e.g. network and internet services create security risks and malfunctioning of equipment. It is the responsibility of all users as well as a council to comply with maintaining the ICT standards by NOT downloading or installing unauthorized software on district owned computers. Any software which needs to downloaded and installed should be approved by the ICT office staff.

In the event that unauthorized software is identified, the ICT Office shall:

1. Immediately uninstall the authorized software.
2. On a routine basis, check and remove unauthorized software, unless the software has legitimate business purpose for the user

The ICT office shall endeavor to work with the User units to ensure any questionable software usage is addressed before removal

6.5 Data backup and Restoration

Users shall ensure that their work files are saved on file servers. For the servers, the following backup policy shall be administered:

1. **Daily Backup:** Every Monday tó Friday at Around 16:15 full backup of the financial and Domain server with all stored information as well as system state and system files are made.
2. **Monthly Backup:** Every last Friday of every month at around 16:15 a full backup of financial server with all stored information as well as system state and system files is made.

3. **Annual Backup:** The yearly backup occurs on the last working day of the year and full back up of the financial server with all stored information as well as system state and system files are made.
4. **Data retention:** Daily backups shall be valid for one full year, whereas yearly backups are kept forever or until disposed of by order.

In addition, a disaster recovery plan (DRP) documenting procedures to protect and recover the management Information systems, Data and ICT infrastructure in the event of a disaster shall be developed and tested

1.1 6.6 Bring your own Device (BYOD)

Due to shortage of ICT equipment, the District Staff may use personal Laptops, Smart phones and Tablets to carry out their official duties.

However, the following rules shall apply:

1. All support issues should be carried out by staff of the ICT Office; if there is need to contact the device manufacturer or the equipment supplier why in use at office premises such contact should be done in the know of the ICT Office.
2. Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.
3. The staff assumes full liability for risks including, but not limited to the partial or complete loss of company and personal data due to an operating system crash, errors bugs, viruses, malware, and or other software or hardware failures or programming errors that render the device unusable.

6.7 ICT Usage by persons with Disabilities (PWDs)

The provision of ICT services should take into consideration the needs of special user group to access services and employment by PWDs. This takes into consideration of the visually motor and auditory impaired user groups. Globally, the development in ICT supports extension of access to all users.

To ensure the universal accessibility of the district ICT systems, the district administration shall:

1. From time to time define the appropriate technology aligned to needs of special users groups.
2. Provide to the staff and end user training and
3. Ensure the provision of the appropriate access for special user groups for all the district web-based systems.

1.2 ICT services support

The ICT Office shall Offer support for the existing ICT systems. This shall include support to all district hardware and software. No support will be given to unauthorized or personal software. Users should supply error code and message of specific problems when logging calls to the ICT Office. No user shall log calls directly to third parties or contractors.

The usage of ICT devices within the district will require a well-planned maintenance plan so as to ensure its safe and proper usage. The relies on the cooperation of all units to ensure proper asset and inventory management on which such maintenance can be achieved through a central coordination role.

This policy applies to all ICT equipment owned by the District LG Administration within the various departments and units.

The ICT Office shall be responsible for:

1. From time to time define and disseminate updated ICT equipment maintenance guidelines to all departments and units.
2. Act as the central point of contact for all district ICT equipment maintenance
3. Provide technical support in the development and implementation of service and maintenance schedules for all District ICT equipment
4. Undertake a periodic assessment in all Departments and Units to ensure compliance with the set maintenance guidelines
5. Maintain records of all ICT equipment including details of manufacturer, warranty and service history.
6. Develop remedial and preventive maintenance schedules on annual basis for all ICT equipment
7. Ensure all ICT equipment is placed within adequate operating environments

8. Ensure all replacements or upgrades of any ICT equipment is undertaken properly.
9. Assessment for repair and certification of ICT related supplies and services
10. Help in providing ICT technical specifications during procurement.

6.9 Software Licensing and Ownership

To ensure that all software in the use by the district administration is properly licensed and owned by the district local government administration.

The following statements shall govern the software licensing and ownership within the district administration:

a) An inventory of all software is maintained;

1. All software is licensed in accordance to the acquisition agreements.
2. All software in usage is properly managed, administered and maintained.
3. All software in usage is approved and aligned to the district information security requirements

b) Any computing equipment that is written off, sold or given to a third party shall have all non-transferable licensed software permanently.

c) Staff shall not be given the ability to download and install software on District equipment

d) Software shall only be used in accordance with its license and duration

e) Software shall only be distributed in accordance with its license agreements

f) Software licensed for official purposes must not be used on personal computing devices

g) All software source code developed with either internal or external resources for District purposes shall be owned by the District and shall be handled over to the District ICT Office for custody.

h) All District Units outsourcing software development that has code restrictions shall ensure usage of appropriate third-party source code escrow agents to ensure continuity.

7. Data Communication

Access to and use of the network, internet and or email systems is provided to employee and council of the district for the purpose of advancing the goals of the district. This access imposes certain responsibilities and obligations on the district staff/council, (full time, part-time and temporary staff) as well as any other companies or individuals (third parties) contracted to do work for the district, or use district ICT resources, and is subject to the District policies. All data, e-mails, e-mail attachments, documents and other electronic information within the network/ e-mail system are the property of District. There should be no expectation of privacy or confidentiality in network use, and e-mail use on the district's systems. The district acting through its managers and supervisors has the capability and the right to view data and e-mail at any time when deemed necessary for District business purposes. The primary purpose for using the District's internet and e-mail connection is solely for advancing the business of the District. This includes, but is not limited to

1. Communication with, and providing services to, clients of the District
2. Conducting the business of the District Departments and Units
3. Communicating with other employees/Councilors for work-related purposes;
4. Gathering information relevant to duties or expansion of expertise

Acceptable use always is lawful, ethical, reflects honesty, and shows restraint in the consumption of shared resources. Users shall refrain from monopolizing systems, overloading networks or computers with excessive data (e.g. music /video files) or wasting computer time, connection time, disk space, printer paper, manuals or other resources. Users may be subjected to limitations on their use of the networks, or other action, as determined by the appropriate supervising authority. User is also expected to cooperate with any investigations regarding the use of computers or activities associated with IT resources. Content of all communications should be accurate. Users should use the same care in drafting e-mail and other electronic as they would for any other written communication. Anything created on as they would for any other written communication anything created on the computer may and likely will be viewed by others as with internal e-mail messages, internal e-mail can be changed by outside parties and forwarded to others without the employees' knowledge or permission. Users must use caution in using internet e-mail and must comply with laws recovery of data stored on desktops is the users' responsibility. Storage only on a PC hard drive disk is a risk in that if the hard drive fails, the data may not be recovered

7.1 Allowable Personal Use

Authorized Users of the district may also use the internet and e-mail for limited personal use. The is a privilege according to staff and not a right which may be limited or removed at any time by management. The District Administration does not accept any liability for any loss or damages suffered by any employee a result of that employee using the District Internet connection for personal use. Occasional, limited, appropriate personal use of the computer system is permitted when the use does not:

1. Interfere with the users work performance (should be infrequent and brief);
2. Interfere with the normal operation of the unit or department;
3. Interfere with any other users work performance or have a negative impact on overall employee productive;
4. Have undue impact on the operation of the computer system;
5. Cause any additional expense or load to the District or unit;
6. Compromise your unit or the District in any way;
7. Violate any other provision of this policy, any other policy guidelines.

In limiting personal use, the District expects employees to exercise the same good judgment that they would use in all work situations.

Inappropriate use

The use of public recourses for personal gain and/or excessive private use, such as but not limited to the items listed below, by any user is absolutely prohibited and punishable by applicable district disciplinary procedures, which may include termination and /or criminal prosecution depending upon the nature severity of the transgression. The term public resource as used in this policy includes not only the un authorized use of equipment, hardware, software or tangible articles, but also the employee time expended in the engagement of the un authorized use while on District time. Examples of unauthorized use of software include streaming music (listening to online music), movie downloads and games. The District Staff shall not:

Use IT resources for personal gain, or to support or advocate for non-District related business.

Create, Distribute, Upload or Download any disruptive, abusive, harassing, threatening, or offensive massages, including offensive comments or graphics about sex, race, gender, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

Use ICT resources, but not limited to, illegal or unlawful purposes or to support or assist such purposes.

Attempt to circumvent or subvert system or network security measures, provide internal network access to any non-users or use your account to gain unauthorized access to eternal network and systems.

Mount an attack on the security of any system (i.e. attempting to hack or introduce viruses into a system).

Use the network to disrupt other network users, service or equipment. Disruptions may include distribution of unsolicited materials propagation of computer viruses and sustained high volume network traffic that substantially hinders others in the use of the network.

Intercept network traffic for any purpose unless engaged in authorized network administrative duties.

Install or use encryption software on any district computer without obtaining written permission from the unit Head and ICT Office. Users may not use encryption keys and encryption pass wards that are unknown to their unit head.

Engage in online fundraising.

Mass- mailing massages without approval from the Unit Head.

Send e-mail about viruses or other warnings about outside computer attacks (these are almost always a hoax, and should be turned over to ICT office for disposition).

Initiate or forward chain letters by e-mail.

Spoof (disguise) your identity or send anonymous e-mail or send e-mail under another employee's name without permission.

Download any non-standard or non-business-related files or software including “free ware” and/or “shareware” programmes unless previously approved.

Load personal Internet Service provider accounts on District owned equipment.

Unless expressly authorized, sending, transmitting, or otherwise disseminating proprietary data, or other mediums, stores such copies on the District systems, or d transmits them over the District network. It is the responsibility of the supervisor, manager and/or unit Head to be aware of how the Districts internet facility is being utilized by his/her staff and ensure that the staff are periodically informed and aware of the IT policies at a minimum on an annual basis

Network Monitoring

All computer applications, programs, data and work-related information created or stored by District employees on District information systems and resources are the property o District. District employees shall have no expectation of privacy in anything they store, send or receive on the District computer systems. District may monitor message or data without prior notice. District is not obligated to monitor email messages. District reserves the right to access and monitor e-mail use and any other computer related transmissions, as well as stored information, created or received by District Users with District Information Technology systems and resources under the following circumstances:

1. Performance monitoring and problem-solving purposes necessary in the course of an investigation for possible violation of District policies.
2. There is reasonable suspicion that a User has committed, or is committing a crime against the District or for which the District could be liable.
3. Random or automated monitoring to ensure that content is incompliance with the business’s established policies.
4. Request for monitoring is made by appropriate authority
5. Required to do so by law

The reservation of this right is to ensure that public resources are not being wasted and to ensure the District’s information systems are operating as efficiently as possible in order to protect the public’s interests. This includes blocking access to certain web sites for which access is deemed to be in conflict with District policy.

7.4 E-mail Records Retention

E-mails and attaché documents are the property of the District, and are subject to District rules stated in this policy. Generally speaking, e-mail messages represent temporary communications that are non-vital and may be discarded routinely. As a result, the content of e-mail system should not be used to transmit sensitive materials (for example, personal matters) that may more appropriately be communicated by written memorandum or personal conservation. However, depending on content of the e-mail messages, it may be considered more formal record and need to be retained pursuant to a Unit's record retention schedule.

Information Security

The District has a comprehensive computing environment that encompasses a broad array of networking, server and client computing platforms as well as the complementary systems software. Users should never consider electronic communications to be either private or secure. E-mail and data could potentially be stored indefinitely on any number of computers, in addition to that of the recipient. Copies of e-mail messages or altered messages may be forwarded to others either electronically or on paper. In addition, email sent o nonexistent or in correct user names may be delivered to persons that the sender never intended.

Each user is responsible for ensuring that his or her use of outside computer and networks, such as the internet, does not compromise the security of the District's Information Systems and networks. This duty includes taking reasonable precautions to prevent introduction and spread of viruses.

Network/Internet Security.

Standards and requirement exist to ensure security and availability of the data and systems. The District's network connects to the Internet through a firewall. Network Devices-prior approval from the ICT Office must be obtained before any of the following activities are attempted. These are not allowed by default:

Connecting any networking devices to the District network.

Usage of modems on individual servers / computers for remote access purposes.

Allowing non-District agencies or entities to access the District network without prior ICT Office approval.

The following activities should only be carried out by ICT Office or its authorized designees:

1. Connecting networking devices to the District network.
2. Interconnecting external networks by routers.
3. To maintain the security of the District network, all the users should ensure that:
4. Their PC's have the most current virus protection installed.
5. Operating systems has all the recommended patches installed
6. Browsers have all the recommended patches installed.

8.2 Anti-Virus Protection

The District network is protected from viruses with help of firewalls, e-mails scanning software and desktop scanning software, however users will still be vulnerable to viruses if the following guidelines are not followed. In some cases, simply reading an e-mail can spread a virus to a User's computer, and from there to many other internal and external District receipts. The District staff shall take prudent measures to scan incoming and outgoing e-mail and attempt to intercept viruses. However, no safeguard is foolproof, and viruses can find their way into District Users' computers from a variety of other ways (e.g, flash disks and internet file transfer). Each User is responsible for taking reasonable precaution to avoid introducing viruses into the District network.

Never open any file or macros attached to an e-mail from unknown, suspicious or untrustworthy sources. Delete these attachments immediately, then "double delete" them by deleting them from "Deleted items"

- ✓ Delete and never forward spam, chain, and other junk e-mail.
- ✓ Never download files from unknown or suspicious sources
- ✓ Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- ✓ Always scan external media for viruses before using it.

Viruses and Laptops: Viruses can gain back door entry via laptops (notebooks) that are normally used outside the official network and may be infected. To eliminate such risks, the following guidelines should be used while using laptops on the District network:

District provided laptops should have the official Antivirus software installed on them. If not installed, please inform the ICT Office.

If connected to the District network, the antivirus signature file should be regularly updated. All other District laptop User s should ensure that they are periodically connected onto the District network for a sustained period of time to get the anti-virus updates.

It is desired that personal laptops not be connected to the District network. If it is total unavoidable then you should:

Ensure that the laptop has antivirus software loaded on it

The signature file for the antivirus software is current

The laptop is scanned for viruses just before it is connected to the District networks.

E-mail Scanning in order to provide further protection for all District Users, the ICT Office has implemented additional measures for electronic scanning of incoming and outgoing e-mal. All e-mall attachments coming to the District will be electronically scanned for key words that are either sexually explicit, or contain known phrases indicative of spam, hoaxes or viruses. Also, the "subject" line in e-mail will be scanned for the same kind of key words. Any e-mail with words or phrases matching the key word list be saved in a quarantine file and copy of the header information will be sent to ICT office who will contact you regarding the rejected e-mail.

It is important to note that e-mail scanning is an electronic comparison a table of inappropriate words and phrases. This electronic scan will reduce offensive materials and make it much more difficult for purveyors of junk e-mail or viruses to interface with normal operations.

1.3 ID's and Passwords

Passwords provide front line protection for user accounts. A poorly chosen password may result in the compromise of the District's entire corporate network. The scope of this policy includes all personnel, council, third parties, who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any District facility has access to the District network or stores any district information. . As such, all are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. Users are responsible transactions made using their passwords. No user may access the computer systems using another User's password or account or portray oneself as another User.

In order to provide appropriate network security, this policy mandates that the District ICT Office to utilize passwords, one that they not used before. Although Users have confidential passwords, this should NOT be construed to mean that application data is the property of the User or that network, internet or e-mail access is for personal confidential communications or that the passwords is to protect the employee's privacy. Users are expected to follow these guidelines when choosing passwords.

Passwords shall remain confidential and should not be printed, stored online or given to others.

1. Passwords shall be changed every 90 days
2. Passwords shall be at least eight characters along

Passwords shall contain characters from at least two of the following three classes:

I. Upper o lower case alphabetic characters
II. Numeric characters
III. Special characters such as %, &, $ etc.

Passwords should not contain your User name or any part of your name

Passwords must not be inserted into e-mail message or any other form of communication

The password should not form a word found in a dictionary

The password shall not be a common usage word such as names of family, pets, friends, Co-workers, fantasy characters etc.

The passwords shall not be your birthday or other personal information such as address and phone number

The password shall not be a computer term, name, command or site, company, hardware or software name.

The password shall not be a word or number patter like aaabbb, query, 123123, etc.

The passwords shall not be any of the above spelled backwards

Third-Party Access

A third-party is any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. A third –party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, trainers and auditors. The policy addresses access to the District network and to our information systems. Contractors or third parties who violate this policy may have their contract revoked. Other legal remedies, including criminal prosecution, may also be pursued if warranted.

8.5 Physical Security

Please follow the guidelines below to avoid security breaches:

Store notebooks and personal affects in a locked drawer, file cabinet, or take them away from desk for extended periods of time, including overnight.

Lock file cabinets when away from desk for extended periods. Do not leave keys in their locks.

Close applications, and turn off your monitor when you leave your desk.

Do not leave portable media such as CDs or floppy disks in drives.

Flash disks can contain lots of confidential information, so do not leave them lying around.

Turn off your computer when you leave or extended periods.

Never write your passwords on a sticky note nor try to hide them anywhere in your office.

Remove printouts from printers before leaving the office.

Locking clips, padlocks shall be used to lock together all the hardware components in a specific office to avoid movement of hardware components by officers from one office to another.

Modern Use Policy

The District has spent considerable money and efforts to secure the network. Communication via modems is allowed only for certain officials and only to transact District business. It is the need for modem communications, prevent outside computer hackers and viruses from destroying computers data both on the network and on PC's and to prevent unauthorized access into the District computerized data file

1.6 Portable Memory

The use of USB flash drivers, small keychain –sized storage devices may be useful and practical under certain circumstances, the unchecked usage of them could pose a data security breach. Therefore, use of portable media at the District is discouraged and requires approval of ICT Office.

Most memory devices of this type are activated simply by plugging them into a USB port, which almost every computer has. From a hardware standpoint, there is nothing to stop unwanted eyes from viewing information on a found or stolen device. Usage of these devices may also cause Users to not utilize the device's native security or backup features (if the device has any, which most don't) other drawbacks and negative aspects of portable memory devices such as USB flash drives include, but not limited to, the following areas of concern:

1.7 Revocation of User Access Rights

Removal of a staffs access account shall be promptly done when an employee leaves employment or is interdicted. The head of department or Unit must inform the ICT Office in time.

Laid-off or terminated employees have no right to the contents of their e-mail messages or data stored in district systems, and should not be allowed access. Should an employee be suspended from duty, the User's access account will de-activate until the suspension has been revoked.

9.0 Software Acquisition and Upgrade

9.1 Software Development

The LG Administrations have over the years been acquiring and developing software to support various functions in an uncoordinated manner. There is therefore, need to achieve a defined common methodology for both the development and acquisition of off- the –shelf software.

The following policy statements shall govern the software development process.

a) The ICT Office shall periodically define the methodology for:

1. Systems and software engineering for both in-house and outsourced development

2. Acquisition of off –the-shelf software
3. Maintenance of existing software

b) All software shall undergo testing and quality assurance before installation in any production environment and this shall ensure provision for:

I. Information classification
II. Usage of the least privilege principal
III. Segregation of roles
IV. Audit trails

c) All software under this policy shall comply with the software Licensing and Cyber security policies

d) All acquired software shall where necessary contain provision for technical support and upgrades.

e) All Department and Units shall where necessary make use of open source software.

f) All Departments and units undertaking the development or acquisition of any software shall ensure compliance to this policy and plan for end user training.

9.2 Software Acquisition

All requests for new technology or the possible upgrading of current technology shall be made in writing to the ICT office. All requests shall be accompanied with confirmation of funding for executing the request. The ICT Office shall do the necessary research on the requested technology. All newly purchased technology shall be received, checked, recorded and installed by the ICT Office. No technology shall be installed by any other employee's contractors or any third parties without the acknowledgment of the ICT Office.

10.0 ICT Skills Capacity Development.

The ICT Office in conjunction with the Human Resource department shall provide guidelines for the process of updating and enhancing User skills in order to keep abreast with rapid changes in ICTs through continuous training.

10.1 Telecommunication Services

Telecommunications services shall be provided to support the communication needs required for smooth operations of the District. In this context, this will include unified communications services based on the existing Local Area Network (LAN) as well as the telephone services.

In order to achieve the smooth running of the telecommunication services the ICT steering committee shall support and promote the usage of unified communications service within the district offices.

11.0 Internal Support

The internal ICT support shall:

1. Design and implement the district wide telephony service and numbering plan to support both intercom services and external calls interconnecting the district headquarters, county, sub-county and parish offices.
2. Design and implement district wide Unified communications services to support new communications channels integrated with e-mail, online meeting s, video conferencing workplace collaboration and seamless file sharing.
3. Ensure proper license usage for all unified communications components
4. Ensure manage and take up responsibility for all infrastructure required to provide a smooth user experience as relates to communications services
5. Provide the required timely technical support through the IT service help desk for all communications related downtime
6. Approve and provide technical assistance for any expansion of the communications services within the district
7. Set and periodically review communications services technical specifications (hardware, consumable, software) as well as configuration and installation guidelines to ensure uniformity for the service provision and compatibility with existing infrastructure
8. Undertake routine maintenance, upgrade and daily monitoring of communications service usage
9. Manage and maintain Service Level Agreements (SLAs) with all suppliers of the required communications services, equipment and software
10. Provide technical guidance and authorization in the design and provision of any radio communications services for the district administration

11.1 User Responsibilities

The Heads of departments and units shall:

1. Ensure the appropriate protection of desk sets. The heads will account for any damaged or stolen telephone desk sets
2. Acquire any telecommunications or communications service centrally through guidance from the ICT Office.
3. Any configuration change, software upgrade or cabling change will only be undertaken by authorized personnel from the ICT Office.

12.0 ICT procurement

Procurement of all ICT equipment and services shall be in conformity with the overall District procurement of goods and services standard as aligned to public procurement and Disposal of Public Assets Act (PPDA).

In addition, the procurement shall comply with the guidelines and standards for acquisition of Information Technology hardware and software for Government Ministries, Departments, Agencies (MDAs) and local government (LG) Administrations. These guidelines provide frame work for procurement of ICT equipment and services with emphasis on standardization of ICT assets, transparency, timely delivery, quality assurance, and value for money as well as compatibility with existing infrastructure and services.

The following roles and responsibilities shall govern the procurement of ICT equipment, software and services within the District.

12.1 District Procurement and Disposal Unit (PDU)

The District PDU shall manage all procurement or disposal activities within the district in line with the PPDA (section 31&32)

12.2 User Departments

The User departments shall

1. Ensure conformity with the procurement policy as implemented by the procurement and disposal Unit
2. Ensure conformity with approved technical guidelines and standards by the Government of Uganda in the procurement of any ICT equipment, software or service.

12.3 The ICT Office Responsible

The office responsible for ICT shall provide technical support to all user departments as provided for below:

- ✓ Provide technical assistance in the development of specifications for any ICT equipment, software or service;
- ✓ Provide technical assistance in identification of the user department ICT needs;
- ✓ Ensure and verify that supplied ICT equipment, software or services comply with the approved ICT specifications, standards and guidelines;
- ✓ Ensure that the installation and configuration of any procured ICT equipment, software or service complies with the approved ICT specifications, standards and guidelines;
- ✓ Maintain an updated inventory of all ICT hardware and software indicating the life cycle
- ✓ Provide support for bulk procurement of commonly used ICT equipment and software as per the business needs.

12.4 Disposal of ICT equipment and software

The District Administration shall:

Define the life-cycle for each category of procured ICT equipment to determine the replacement cycle;

Disposal of retired ICT equipment shall comply with the PPDA Act.

Software disposal will rely on the system support cycle of the software developer company.

13. Social Media Guidelines

Social media can be referred to websites and applications that enable users to create and share electronic content or to participate in social networking after subscription. The following guidelines are intended to guide and enhance the usage of social media by the district officials. Adherence to these guidelines will enhance the on line personal and professional reputations of the district staff.

1.4 Official District Social Media Accounts

1. Only the official district social media pages shall display the district logo, emblem and symbols;
2. Only staff authorized by the District Administration shall be allowed to make postings on the district official social media pages

3. Any information shared across the official social media pages shall comply with the district policies.
4. Any information shared across the official social media sites should not make reference to any biased statements on matters such as politics, religion, race, gender, sexual orientation, or statements that contain obscenities or vulgarities inter alia;

1.2 Personal social media accounts for staff

The district staff shall adhere to the following while running their personal social media sites

Respect the laws relating to copyright and other intellectual property rights, defamation, privacy and other applicable laws.

Not portray colleagues in an unfavorable light in respect of matters including, but not restricted to religion, gender, sexual, preference, nationality or disability;

Maintain adherence to the overall public service confidentiality and information non –disclosure agreements;

Not make reference to any staff or client's personal information

13.0 Policy Enforcement

The ICT Office has direct responsibility for maintaining and guiding implementation of policy.

District employees as well as district councilors who violate this policy may have their access removed and may be subject to disciplinary action up to and possibly including termination.

District employees as well as district councilors who violate this may have their access removed and may be subject to disciplinary action up to and possibly including germination.

In addition, contractors or other third parties who violate this policy may have their contract revoked. Other legal remedies, including criminal prosecution may also be pursued if warranted sanctions for inappropriate use of the district's network resources or failure to comply with this policy may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing and networking resources and facilities

2. Disciplinary action according ~~g~~ to applicable policies and regulations;

Legal action according to applicable legislation and contractual agreements. The rules and guidelines require strict adherence. Failure to conform and comply with these rules and guidelines will subject individuals to appropriate disciplinary action commensurate with the severity of the infraction and may result in disciplinary actions up to and including termination as well as criminal prosecution.

14.0 Monitoring and Evaluation

All ICT systems, as with all other assets are the property of the District. The District administration, therefore reserves the right to monitor these systems to ensure compliance with this policy. The monitoring of the ICT system activities shall be carried out in a manner that respects the rights and legitimate interests of those concerned.

Users of the District's ICT systems should be aware that their activities can be monitored and they should not have any expectation of privacy. In order to maintain their privacy, users of the district's ICT resources should avoid storing information on these systems that they consider private. By using the District's ICT systems, users expressly consent to the monitoring of all their activities within the District's ICT systems.

During the implementation of this policy, the District Administration will ensure that there is continuous monitoring and evaluation (M&E) of the policy for efficiency, accountability and transparency. The M&E will be carried out by the ICT steering committee and other relevant Government MDAs led by the Ministry of ICT and National Guidance.

The ICT steering Committee shall:

1. Develop appropriate strategies for M&E of this policy

2. Carry out annual evaluation on the implementation of the policy; and

3. Define short, medium and long-term interventions based on the outcomes of the M&E reports.

15.0 Policy Review

This policy will be regularly reviewed and amended after every three years to ensure it remains relevant and effective in meeting the policy objectives. The responsibility for the ongoing review resides with the ICT Office .in conjunction with the District ICT steering Committee. Any proposals during intervening period should be submitted to the ICT Office. Any changes to this policy shall be communicated to all users of the district's ICT systems.

16.0 Glossary

Application: refers to software programs developed to execute certain specific tasks such as Academic Records Information System, Financial Information System and like

Appropriate Use: refers to use that is consistent with the teaching, learning, research, District-based consultancy, and administrative objectives of the District and with the District's Guiding Ethical principles. It includes incidental use by persons authorized to use District ICT facilities and services

Authorized User: refers to any member of the district staff allowed to use the district's ICT facilities and services.

Attachments: Files created in other applications (such as Ms-word, MS-Excel) or pictures that are transmitted via e-mail.

Back up: refers to procedures to replicate data such that the data can be used for recovery in the event of a disaster.

Bandwidth: refers to the rate of data transfer in an electronic communication system.

Bring Your Own Device (BYOD): refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access company information and applications.

Communication: refers to exchange of information and data between individuals and group through electronic media

Electronic Information: refers to any information or recorded, either mechanically, magnetically, or electronically, with the District ICT facilities and services, including data, messages, music, computer software, films, video, etc.

E-Mail: An electronically transmitted message, along with attachments and any information appended by the e-mail system.

E-Mail System: Computer hardware and software system that allows computer/tablets/smart phones Users to send, receive and store messages documents and files with other individuals or groups of people over an internal network or the internet.

Encryption: A means of coding messages so they appear to be random characters. Encryption has two benefits. First, it prevents disclosure of sensitive information to unauthorized third-parties. Second encryption allows for verification of information sent.

Freeware/Open Source: Software that is offered at no cost, which is copyrighted so that one can't incorporate its programming into anything one may be developing.

Hacking: The unauthorized attempt or entry into any other computer system.

Hardware: refers to equipment and ICT component such as computer, printer and etc

ICT: refers to all information and communications technology hardware and software, data and associated methodologies, infrastructures and devices that are owned, controlled or operated by the District

ICT facilities and services: Refers to any information resources provided by the District to assist or support teaching, learning, research and administrative activities. This includes, but is not limited to, physical spaces designated for teaching, study or research, all digital and electronic information storage, software and communication media devices, including, but not limited to, telephone, mobile phones, wireless or computer networks, computer workstation equipment including laptops, personal digital assistants, electronic e-mail system, internet, intranet and extranet. ICT facilities and services cover all types of ICT facilities owned or leased by the District, ICT services provided by the District and computer equipment owned or leased by Users which are used to connect to the District networks and / or the Internet

Internet: A world wide web or computer network through which you can send a letter, chat to people electronically or search for information on almost any subject you can think of. Quite simply it is a "network of computer networks"

Internet Browser: An application that displays web sites and other applications found on the internet. Internet Explorer is an example of Internet Browser. This type of client software accesses the World Wide Web and lets you drift from link to link without having to have a purposeful search.

Risk: Those factors that could affect confidentiality, availability, and integrity of the District's key information assets and systems. The District is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

Shareware: software that is distributed free on "trial basis" with the understanding that the User my need to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date.

Software: Refers to computer programs used to execute specific tasks such as office automation software, graphics software among others.

Third-Party: Any individual from an outside source (contracted or otherwise) who require access to our information systems for the purpose of performing work. A third –party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and trainers.

Users: Any individual who has access to our information systems for the purpose of performing work. Users consist of, but are not limited to employees, councilors, third parties etc.

Virus: refers to a program or code inserted in a computer without the knowledge of the computer owner and executing operations without the knowledge of the computer owner.

Website: refers to location connected to the Internet that maintains one or more World Wide Web (www) pages for any entity such as District to enable users to access and store information about the entity

World Wide Web (www): A hypertext-based distributed information system for linking databases, servers, and pages of information available across the internet.

References

The computer Misuse Act (2011) accessible at http://www.ict.go.ug/resource/computer-misuse-act.

The Electronic Transactions Act (2011) accessible at http://www.ict.go.ug/resource/electronic-transactions-act The Access to information Act (2005) accessible at http://www.ulrc.go.ug/content/access-information-act-2005

Guidelines and standards for acquisition of information Technology hardware and software and software for Government (LG) Administrations accessible at https://www.nita.go.ug/publication/guidelines-and-standards-acquisition-it-hardware-software-mdas

Recommended Minimum hardware software standards NITA-U accessible at https://www.nita.go.ug/publication/guidelines-and-standards-acquisition-it-hardware-software-mdas.

Lemmetti, Juha, and Samuli Pekkola. "Enterprise architecture in public ICT procurement in Finland." Electronic Government and Electronic Participation: Joint Proceedings of Ongoing Research and Projects of IFIP WG 8 (2014): 227-236.

Gordineer, J. (2003). Blended threats: A new era in anti-virus protection. Inf. Secur. J. A Glob. Perspect., 12(3), 45-47.

Saad, Y., & Schultz, M. H. (1989). Data communication in parallel architectures. Parallel Computing, 11(2), 131-150.

Vorisek, Jiri, Jaroslav Jandos, and Jiri Feuerlicht. "SPSPR model-framework for ICT services management." Journal of Systems Integration 2, no. 2 (2011): 3-10.