



THE REPUBLIC OF UGANDA

## **MBARARA DISTRICT LOCAL GOVERNMENT**

---

# **INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY MANUAL**

**SEPTEMBER 2021**

## TABLE OF CONTENTS

TITLE: INFORMATION AND COMMUNICATIONS TECHNOLOGY STRATEGY .....	4
TITLE: INFORMATION CLASSIFICATION .....	6
TITLE: USAGE AND MANAGEMENT OF INFORMATION COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE .....	9
TITLE: ICT ACCEPTABLE USE POLICY.....	11
TITLE: ICT PROCUREMENT .....	13
TITLE: INFORMATION SECURITY .....	16
TITLE: SOFTWARE PLANNING AND DEVELOPMENT .....	21
TITLE: BRING YOUR OWN DEVICE .....	24
TITLE: ICT PROJECT MANAGEMENT .....	26
TITLE: DATA PROTECTION AND PRIVACY .....	28
TITLE: POLICY MANAGEMENT FRAMEWORK .....	31

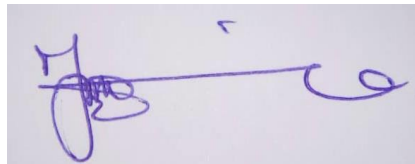
## **FOREWORD**

Mbarara district local government has embraced developments in ICT. The objective of this policy is to guide the district to move towards realizing the district objectives in particular and the national Objectives in General.

The District recognizes the role of information Technology in planning, budgeting, project implementation, monitoring and evaluation of performance. As such, efforts have been made to equip and support the use and development of ICT initiatives in the district.

All staff are called upon to effectively use this policy to deliver effectively and efficiently.

Signed:

A handwritten signature in blue ink, appearing to be 'Tumwesigye Didas Tabaro', written on a light-colored background.

---

Tumwesigye Didas Tabaro  
District Chairperson

Date: 14<sup>th</sup> November, 2021

## ACKNOWLEDGEMENT

Information and Communications Technology (ICT) is a key enabler for increased efficiency and productivity for Mbarara District Local Government. It is within this regard that this ICT Policy Manual has been developed to ensure alignment with the National related ICT Laws, Regulations, Standards and Guidelines. All staffs are required to ensure compliance to this Policy.

Signed:



---

Kasagara Edward

Chief Administrative Officer

Date: 14<sup>th</sup> November, 2021

**TITLE: INFORMATION AND COMMUNICATIONS TECHNOLOGY STRATEGY**

Doc ID: ICTP/01

Policy: Mbarara District Local Government shall utilize Information and Communications Technology (ICT) to enhance its productivity

Purpose: To ensure that the use of ICT increases overall productivity and enhances risk management and performance as well as achieve positive returns on the investment in technology.

Scope: This applies to Mbarara District Local Government

Responsibilities:

- a) The District Council shall be responsible for approving Mbarara District Local Government ICT Strategy
- b) Chief Administrative Officer is responsible for:
  - i. presenting Mbarara District Local Government ICT Strategy to Council for approval
  - ii. ensuring that Senior Management leads the implementation of the strategy
  - iii. providing strategic leadership, management and supervision in implementation of the Strategy
  - iv. ensuring that the District has in place an ICT unit with competent Information Technology (IT) professionals in accordance with the recommended structure as per the Institutionalization of Information and Communications Technology (ICT) Function in Ministries, Departments, Agencies and Local Governments (MDAs/LGs)
- c) Senior Management is responsible for;
  - i. implementing the ICT Strategy
  - ii. Periodically reviewing the District's ICT Strategic plan
- d) The officer charged with the responsibility of Heading Information Technology (IT) is responsible for developing the ICT Strategy, reviewing the Plan with Senior Management, overseeing implementation of the Plan and periodically verifying that the ICT Strategy continues to meet the District's requirements.
- e) All staff should comply with the implementation of the strategy.

Definition:

a) Risk: Possibility of loss or injury to Mbarara District Local Government

PROCEDURE:

1.0 STRATEGY PLANNING

- 1.1 The officer charged with the responsibility for ICT shall develop the ICT Strategic Plan in coordination with the District's departments. The Strategic Plan shall ensure that all ICT related initiatives are well defined and measurable which shall be included in a three-year cycle. In addition, the ICT Strategic Plan shall be formally submitted to the National Information Technology Authority, Uganda (NITA-U) for review and to ensure compliance with National IT standards
- 1.2 Once NITA-U has reviewed and officially provided clearance, the ICT Strategic Plan shall be ready for submission to the District's Senior Management for further review
- 1.3 Senior Management will review the ICT Strategic Plan and recommend the same to the Chief Administrative Officer for on-ward submission to Council for approval. Once the Council has approved, the Chief Administrative Officer shall communicate the approved strategy to all responsible departments for implementation.
- 1.4 The responsible ICT officer shall coordinate the implementation of the strategy to all departments.
- 1.5 In line with the above (1.3), Senior Management shall ensure that the ICT projects are budgeted for within each Financial Year

2.0 STRATEGY REVIEW

- 2.1 At least once a year, the officer charged with responsibility for ICT shall cause a meeting to review the strategy to ensure that it continually meets the District's objectives
- 2.2 If the results of the review meeting include updating the Strategy, the recommendations shall be submitted first to NITA-U and then Senior Management for review and submission to the District Council for approval
- 2.3 After the District Council's approval, the officer charged with the responsibility of ICT shall ensure that the Strategy is updated and disseminated to all responsible departments to initiate implementation

**TITLE: INFORMATION CLASSIFICATION**

Doc ID: ICTP/02

Policy: All information shall be assigned an appropriate security classification

Purpose: To define measures for classifying, labelling and handling information

Scope: This applies to all information (created, collected, stored )or processes by (staff, contractors and third parties) in both electronic and non-electronic formats.

Responsibilities:

- a) Information owners are responsible for appropriate classifying information
- b) Information Custodians are responsible for labelling data with the appropriate classification and applying required and suggested safeguards
- c) Information users are responsible for complying with the information use requirements
- d) Senior Management is responsible for the approval of the Information Classification Procedures and guidelines

Definitions:

- a) Information owner: a person who in their role has the operational authority for specified information and responsibility for establishing the controls for its creation, collection, processing, dissemination and disposal
- b) Information custodian: a person who in their role is responsible for overseeing and implementing the necessary safeguards to protect information and/or information assets aligned to the level classified by the Information Owner
- c) Information Users: a person who makes use of information in any way to complete a task

## PROCEDURE:

### 1.0 PREPARING THE INFORMATION CLASSIFICATION PROCEDURES AND GUIDELINES

1.1 The officers responsible for the administration of the District's information records shall develop the Information Classification Procedures and Guidelines aligned to Government of Uganda legal requirements and the Security Standard No. 3 on Security Classification as per the National Information Security Framework. These should be developed as per security classification and business impact levels indicated below:

<b>Classification Level</b>	<b>Notes</b>	<b>Impact Level</b>	<b>Business Impact</b>
Unclassified	Routine Information and communications with the public	0	Trivial
Unclassified – Personal	Information dealing with identifiable individuals such as health records, medical history, etc	1	Low
Official	Information records and assets in the possession or control of the institution	2	High
Secret	Highly sensitive information that if compromised could have extremely serious consequences on the institution	3	Extreme
Top Secret	Enormously sensitive information that if compromised could have catastrophic consequences on the institution	4	Catastrophic

1.2 The Information Classification Procedures and Guidelines should at the minimum include guiding principles, information marking, handling and control, transmission/ carriage of classified information and destruction



1.3 Senior Management shall evaluate the Information Classification Procedures and Guidelines and forward to the Chief Administrative Officer for on-ward submission to District Executive Committee for approval.

## 2.0 IMPLEMENTING THE INFORMATION CLASSIFICATION PROCEDURES AND GUIDELINES

2.1 The officer designated by the Chief Administrative Officer shall communicate the approved Information Classification Procedures and Guidelines to all staff for implementation.

2.2 Heads of Department shall ensure that the Information Classification Procedures and Guidelines are implemented in their area of responsibility

## 3.0 MONITORING AND REVIEWING INFORMATION CLASSIFICATION PROCEDURES AND GUIDELINES

3.1 The officer designated by the Chief Administrative Officer shall monitor and report at least once a year to Senior Management on the status of implementation of the Information Classification Procedures and Guidelines

3.2 Any significant deviation from the Information Classification Procedures and Guidelines shall require that Senior Management consider such changes for approval. In addition, any change from Public Service on Government of Uganda information classification categories shall cause an update of the District's Classification Guidelines

## 4.0 INFORMATION CLASSIFICATION PROCEDURES AND PLAN UPDATE

4.1 After any review of the Information Classification Procedures and Plan, the officer designated by the Chief Administrative Officer shall be responsible for communicating the updates for staff, contractors and third parties to implement

## **TITLE: USAGE AND MANAGEMENT OF INFORMATION COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE**

Doc ID: ICTP/03

Policy: Information Communications Technology (ICT) infrastructure and related services should be provisioned in compliance with National ICT Standards and Industry Best Practice

Purpose: To define measures for the operation, management, usage and maintenance of ICT infrastructure and related services

Scope: This applies to all ICT infrastructure and related services

### Responsibilities:

- a) The Unit charged with Responsibility for ICT shall ensure that the measures provided within this policy (ICTP/03) are implemented and annual status reports are submitted to the Chief Administrative Officer
- b) All staff should ensure compliance

### Definition:

- a) Information Communications Technology: the use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data

### PROCEDURE:

#### 1.0 DEVELOPING THE DISTRICT'S USAGE AND MANAGEMENT OF ICT PLAN

1.1 The unit responsible for ICT within the District shall study the Guidelines for Operation, Usage and Management of Information Technology in Government MDAs and Local Governments' to develop their institutional usage and management of ICT Plan. The Guidelines cover the following areas:

- a) Operation of ICT Equipment
- b) Management and Usage of ICT Infrastructure
- c) Website Management and Usage
- d) Information Technology Equipment Rooms
- e) ICT Equipment and Software Management Guidelines
- f) Maintenance and Repair of ICT Equipment
- g) Human Capacity Development

1.2 The Unit responsible for ICT shall submit the District's usage and management of ICT Plan to the Chief Administrative Officer for on-ward submission to the District Executive Committee for approval.

## 2.0 IMPLEMENTING THE DISTRICT'S USAGE AND MANAGEMENT OF ICT PLAN

2.1 The officer charged with the responsibility for ICT shall initiate implementation upon approval by the District Executive Committee.

## 3.0 UPDATING THE DISTRICT'S USAGE AND MANAGEMENT OF ICT PLAN

3.1 After any review of the 'Guidelines for Operation, Usage and Management of Information Technology in Government MDAs and Local Governments' by NITA-U, the officer designated as responsible for ICT shall be responsible for updating their District's plans and communicating the updates to all concerned parties for implementation.

**TITLE: ICT ACCEPTABLE USE POLICY**

Doc ID: ICTP/04

Policy: The use of computers, equipment, e-mail, internet and related services used by Mbarara District Local Government employees, temporary staff and contractors shall be governed by a mandatory Information Communications Technology (ICT) Acceptable Use Policy

Purpose: To define specific standards regarding the use of computers, email, internet and related services provided by Mbarara District Local Government to its employees, temporary staff and contractors

Scope: This policy applies to all Mbarara District Local Government employees, temporary staff, contractors, Intern students, MDA's staff and consultants on official duty with access to Computers, E-mail, Internet and related services provided by the District during the course of their service to Mbarara District Local Government.

Responsibilities:

- a) All Mbarara District Local Government employees, Temporary staff and contractors are responsible for knowing and adhering to this usage policy
- b) Senior Management is responsible for enforcing this policy  
The Human Resources Department is responsible for communicating the policy to all new employees and ensuring that each employee signs the appended the ICT Acceptable Use Policy upon recruitment
- c) The officer charged with responsibility for ICT is responsible for monitoring compliance of the implementation of the ICT Acceptable Use Policy.

## PROCEDURE:

### 1.0 ACCEPTABLE USE – COMPUTERS, E-MAIL AND INTERNET

- 1.1 The officer charged with responsibility for ICT shall submit the ICT Acceptable Use Policy extract to the Human Resources Department in order to ensure that each employee individually acknowledges by signing a copy
- 1.2 All Departments shall ensure that all the staff in their area of responsibility have signed commitment to the ICT Acceptable Use Policy
- 1.3 Any user violating this policy and guidelines while using Mbarara District Local Government issued ICT resources shall be subjected to disciplinary actions as stated in the District's Human Resource manual or procedures.

### 2.0 ICT ACCEPTABLE USE POLICY REVIEW

- 2.1 At periodic intervals (once a year – recommended), the officer charged with responsibility for ICT shall review the ICT Acceptable Use Policy to assess whether it continues to meet its purpose and report on the same to Senior Management
- 2.2 Senior Management shall recommend for approval of any changes where deemed necessary.

**TITLE: ICT PROCUREMENT**

Doc ID: ICTP/05

Policy: All Information Communications Technology (ICT) related hardware, software, services and consultancies shall be procured in line with Mbarara District Local Government business requirements and National ICT Standards

Purpose: To provide guidance with respect to the procurement of ICT related hardware, software, services and consultancies that support Mbarara District Local Government business needs.

Scope: This procedure applies to any ICT related hardware, software, services and Consultancies.

Responsibilities:

- a) The Chief Administrative Officer is responsible for ensuring that all ICT related procurements are carried out in line with the National Information Technology Authority, Uganda (NITA-U) ICT Approval Process
- b) The Units responsible for ICT are responsible for the development of specifications and terms of reference for all ICT related procurements in line with the following:
  - Government of Uganda 'Guidelines and Standards for Acquisition of IT Hardware & Software for Ministries, Departments, Agencies and Local Governments' published by NITA-U
  - NITA-U (Certification of IT Providers and Services) Regulations 2016 - SI No. 69 of 2016
- c) The Procurement and Disposal Unit is responsible for managing the procurement process for ICT outsourced services as per the Public Procurement and Public

Disposal (PPDA) regulations

- d) Contracts Committee is responsible for providing oversight over the procurement process as prescribed in Clause 12 of the Public Procurement and Disposal of Public Assets (Procuring and Disposing Entities Regulations, 2014).

## PROCEDURE:

### 1.0 GUIDANCE FOR OUTSOURCING OF AN IT SERVICE

1.1 Departments should ensure that any ICT service identified for outsourcing must meet one or more of the following aspects:

- Serve an institutional business need
- Enhancing a service resilience (availability and efficient fault response)
- Leads to cost advantages (reduced capital and operational costs) while maintaining quality
- Increase efficiency and productivity of the affected service
- Provide access to skilled or specialized resources
- Managing risk through risk sharing
- Provide Access to the most current technology
- Support all round clock monitoring of an IT service environment

1.2 The Unit responsible for ICT shall make prior review of specifications for all ICT related procurements

1.3 All outsourced services shall include where applicable a section on risk management to reduce the overall risk exposure to Mbarara District Local Government

- 1.4 The Unit responsible for ICT shall periodically review Mbarara District Local Government's IT Outsourcing agreements and ensure that they support the institution's objectives
- 1.5 Responsibility for maintaining effective internal controls over financial reporting in conjunction with outsourced activities rests with the responsible department.



## 2.0 SELECTING A SERVICE PROVIDER/ SUPPLIER

2.1 Service providers/ suppliers shall be selected in accordance with PPDA procedures, ICT Approval Process and Certification of IT Providers and Services.

## 3.0 ARBITRATION

3.1 All Mbarara District Local Government ICT outsourced service contracts and agreements should include a section for arbitration to resolve disputes that may arise during the contracting period.

## 4.0 VENDOR RELATIONSHIP MANAGEMENT

4.1 The Unit responsible for ICT shall maintain a register of all ICT outsourced services

4.2 All ICT outsourced services shall be evaluated on a schedule as prescribed in the contracts. The overall principle is that all ICT outsourced services shall be regularly evaluated on the basis of performance requirements (measured against Service Level Agreements) and conformance to NITA-U ICT Standards Catalogue.

## 5.0 ICT PROCUREMENT POLICY REVIEW

5.1 At periodic intervals (once a year – recommended), the officer charged with responsibility for ICT shall review the ICT Procurement Policy to assess whether it continues to meet its purpose and report on the same to Senior Management

5.2 Senior Management shall recommend for approval any changes where deemed necessary.

**TITLE: INFORMATION SECURITY**

Doc ID: ICTP/06

Policy: All Information Communications Technology (ICT) and information assets shall be maintained in a secure and trusted manner.

Purpose: To provide measures that maintain the confidentiality, integrity and availability of all ICT and information assets owned by Mbarara District Local Government

Scope: This procedure applies to all ICT and information assets owned by Mbarara District Local Government

Responsibilities:

a) The Chief Administrative Officer is responsible for ensuring that:

- All ICT related risks have been managed to acceptable levels as required of the National Information Security Framework (NISF)
- At least one staff member of the Unit responsible for ICT is assigned information security responsibilities

b) The Unit responsible for ICT is responsible for:

- The implementation, maintenance and monitoring of the appropriate information security controls as well as ensuring compliance to the National Information Security Framework (NISF)
- continuously monitoring threats and implementing attendant mitigating controls

c) All staff are responsible for complying with this policy

PROCEDURE:

1.0 ICT RISK MANAGEMENT

- 1.1 The Unit responsible for ICT shall at regular intervals (at least once every six months) conduct a threat and vulnerability assessment of the District's ICT Infrastructure and related services. Findings of this assessment shall be recorded in an ICT Risk Register and submitted to the Chief Administrative Officer
- 1.2 The Head of the Unit responsible for ICT shall ensure that mitigation measures are developed and implemented to address any risks arising from the threat and vulnerability assessment. The officer shall maintain documentary evidence
- 1.3 The Head of the Unit responsible for ICT shall ensure that once every year, an external NISF compliance assessment of the District is carried out by the National Information Technology Authority, Uganda.

## 2.0 MALICIOUS CODE PREVENTION

- 2.1 Licensed malicious code prevention software such as anti-virus shall be installed on all computers, laptops and servers
- 2.2 Such software should be configured in a way that end users cannot disable its functionality
- 2.3 The Unit responsible for ICT shall ensure that all anti-virus software installations receive daily updates and are configured to scan hosts at periodic intervals. Centralized administration and deployment of anti-virus updates is recommended
- 2.4 Only staff that belongs to the Unit responsible for ICT shall have rights to install software on all Mbarara District Local Government computers, laptops and servers.

## 3.0 IDENTIFICATION AND AUTHENTICATION

- 3.1 All Mbarara District Local Government authorized users shall have a unique identifier (username) and password
- 3.2 The Human Resource department shall maintain an access form which staff will utilize to request access
- 3.3 All user access should be role based with the least privileges
- 3.4 All user access shall be suspended after
  - five (5) consecutive failed logon attempts
  - unauthorized or illegal activity
  - sixty (60) days of account inactivity
- 3.5 The Unit responsible for ICT shall maintain an access control system (centralized deployment recommended such as Active Directory) to authenticate each user and prevent unauthorized use
- 3.6 The Unit responsible for ICT shall audit the list of authorized users at least once every quarter
- 3.7 Human Resource departments shall notify the Unit responsible for ICT to disable access to officers that have been transferred or no-longer employed at Mbarara District Local Government
  
- 4.0 SERVER SECURITY
- 4.1 All servers deployed in the District's ICT environment shall be protected against malicious cyber attacks
- 4.2 Server configuration shall be based on the appropriate security needs backed up by an IT risk assessment
- 4.3 Servers shall be physically located in a secure and monitored area and protected against unauthorized access
- 4.4 The officer charged with responsibility for ICT shall approve all installation and configuration changes
- 4.5 Configuration information for each server shall be backed up and securely stored

- 4.6 All operating systems and software installed on servers shall be licensed
- 4.7 The Unit responsible for ICT shall ensure daily monitoring of the Server resources such as storage and compute utilization
- 4.8 All default server credentials (usernames and passwords) should be disabled and changed during implementation

## 5.0 NETWORK SECURITY

- 5.1 The District's network shall be configured in a manner that supports network segregation. As a principle, sensitive ICT devices such as routers, switches and servers shall be placed in a segment separate from end users
- 5.2 The District shall have in place a firewall to protect its network perimeter against malicious cyber attacks
- 5.3 The network design and implementation shall be documented, frequently updated and securely stored
- 5.4 All structured cabling for the network must be implemented in compliance with the minimum requirements in the 'Standards for Structured Cabling for Government Ministries, Departments, Agencies and Local Governments' published by NITA-U
- 5.5 All access to the Network must be controlled by the Unit responsible for ICT
- 5.6 Appropriate measures must be deployed to monitor the performance and health of the network
- 5.7 All default login credentials (passwords and usernames) for network devices should be changed during implementation
- 5.8 All remote access to the network must be controlled by the Unit responsible for ICT

## 6.0 PATCH MANAGEMENT

- 6.1 All operating systems and applications on the District's computers, laptops, servers, network devices shall be maintained at manufacturer released updates with minimum n-1 versioning. Exceptions must be approved by the Chief Administrative Officer backed up by justification and risk assessment
- 6.2 Patches shall be tested and implemented in a timely manner (centralized patch management is highly recommended)
- 6.3 The officer charged with responsibility for ICT shall be responsible for reviewing and approving any patch installation
- 7.0 INCIDENT MANAGEMENT
- 7.1 All ICT incidents must be reported, investigated and resolved by the unit responsible for ICT.
- 7.2 The ICT Unit shall maintain an updated incident management procedure in line with the NISF and communicate the same to all staff
- 7.3 The ICT Unit shall maintain active subscription to the Uganda National Computer Emergency Response Team and Coordination Center at NITA-U in order to keep abreast with the latest Information Security advisories and alerts
- 8.0 BACKUP
- 8.1 All critical information assets shall be backed up at regular intervals and securely stored
- 8.2 Enterprise information assets shall be hosted at the National Data Center at NITA-U
- 8.3 The ICT Unit shall ensure that they maintain an updated backup schedule which must entail the following minimum areas:
  - assignment of responsibility to back up the identified critical information assets
  - list of information assets and data to be backed-up
  - types of backup and frequency

- testing and restoration procedures
- data retention as per the relevant institution's legal requirements
- secure storage

## 9.0 DISPOSAL OF ICT EQUIPMENT

9.1 All ICT equipment shall be sanitized before disposal

9.2 The ICT Unit shall ensure they maintain an updated procedure for disposal of ICT equipment as per the relevant PPDA regulations

## 10.0 INFORMATION SECURITY AWARENESS AND EDUCATION

10.1 All staff shall be made aware of information security threats in order to increase their level of cyber defence knowledge

10.2 The ICT Unit shall ensure they maintain and implement an updated information security awareness and education plan for all staff

10.3 Information Security Awareness and Education training should be mandatory during on-boarding/ induction of new staff members

## 11.0 INFORMATION SECURITY POLICY REVIEW

11.1 At periodic intervals (once a year – recommended), the officer charged with responsibility for ICT shall review the Information Security Policy to assess whether it continues to meet its purpose and report on the same to Senior Management

11.2 Senior Management shall recommend for approval any changes where deemed necessary.

## **TITLE: SOFTWARE PLANNING AND DEVELOPMENT**

Doc ID: ICTP/07

Policy: All software must meet the specific District business needs

Purpose: To provide measures that ensure that all software meets the business requirements of Mbarara District Local Government

Scope: All software products owned by Mbarara District Local Government  
Responsibilities:

- a) The Unit responsible for ICT is responsible for ensuring that business requirements and design requirements address the needs of Mbarara District Local Government
- b) All staff are responsible for complying with this policy

### **PROCEDURE:**

#### **1.0 OFF THE SHELF SOFTWARE**

1.1 The user department shall develop the business case for the proposed software

1.2 The ICT Unit shall provide support to all user departments to ensure that clear user requirements and specifications have been developed

1.3 The planning for 'Off the Shelf Software' shall take into consideration the following minimum aspects:

- Licensing
- support and maintenance
- access to security releases

1.4 Procurement shall be done in line with ICTP/05 on ICT Procurement



## 2.0 IN-HOUSE DEVELOPED SOFTWARE

- 2.1 The unit responsible for ICT shall provide support to the user department to ensure that the business analysis is carried out in order to develop clear functional requirements of the desired software, service or solution
- 2.2 The unit responsible for ICT shall ensure that the intended software does not duplicate similar efforts in already existing Government of Uganda software products. In-case duplication arises, the unit responsible for ICT shall contact the National Information Technology Authority, Uganda to request access to the desired software product for re-use
- 2.3 The software functional requirements shall be the basis for the software design. The software design shall as such transform the functional requirements into technical requirements taking into consideration aspects of clear process flows, data integration and data models. Software must be compliant to the National ICT Software Interoperable standards
- 2.4 All enterprise software should be designed to operate in a virtualized environment within the National Data Center at NITA-U
- 2.5 In case such software requires data from another Government Agency, such access shall be obtained through the National Systems Integration Platform at NITA-U
- 2.6 Mbarara District Local Government shall ensure presence of competent in house system developers where possible that shall adhere to best practice of development, testing, documentation and support
- 2.7 Mbarara District Local Government shall retain copyright ownership of in house developed software

## 3.0 OUTSOURCED SOFTWARE DEVELOPMENT

- 3.1 The user department shall document the business case for the software product

- 3.2 The unit responsible for ICT shall ensure that the requested software functionality does not duplicate existing software projects
- 3.3 The Procurement for outsourced software development shall be done in line with ICTP/05 on IT Procurement
- 3.4 In case such software requires data from another Government Agency, such access shall be obtained through the National Systems Integration Platform at NITA-U
- 3.5 The unit responsible for ICT shall ensure that the contract clearly stipulates copyright ownership of the software and training of both technical and end users

#### 4.0 SOFTWARE PLANNING AND DEVELOPMENT POLICY REVIEW

- 4.1 At periodic intervals (once a year – recommended), the officer charged with responsibility for ICT shall review the Software and Development Policy to  
assess whether it continues to meet its purpose and report on the same to Senior Management
- 4.2 Senior Management shall recommend for approval any changes where deemed necessary.

**TITLE: BRING YOUR OWN DEVICE**

Doc ID: ICTP/08

Policy: Mbarara District Local Government shall develop and maintain a set of rules governing the use of employee-owned laptops, tabs, PCs and smartphones to reduce risk exposure

Purpose: To communicate specific standards and guidelines regarding the use of personal devices to conduct Mbarara District Local Government' business.

Scope: This procedure applies to all Mbarara District Local Government employees and guests

Responsibilities:

- a) All employees are responsible for being aware of, understanding and adhering to this Bring Your Own Device (BYOD) Policy
- b) The officer charged with responsibility for ICT shall communicate the BYOD policy to employees
- c) Senior Management is responsible for reviewing and recommending to the Chief Administrative Officer the BYOD Plan

Definition:

- a) Bring Your Own Device (BYOD): using one's personal mobile phone, PC, tablet or other personal electronic device to conduct official business.

PROCEDURE:

## 1.0 BYOD PLAN DEVELOPMENT

1.1 The unit responsible for ICT shall develop the BYOD Plan and Procedures taking into consideration the following minimum aspects:

- Roles and responsibilities
- Education, use and operation of BYOD devices
- Security risks and technological measures for app containerization, remote wiping for staff using personal owned devices for accessing the District's systems and services
- Applications that may run on BYOD devices
- Support provided for BYOD devices
- Procedures for using personal laptops on the institution's Local Area Network and Wi-Fi Access

1.2 The unit responsible for ICT shall present the Plan to Senior Management for review and recommendation to the Chief Administrative Officer for onward submission to District Executive Committee for approval.

## 2.0 BYOD PLAN IMPLEMENTATION

2.1 Upon approval:

- a) The officer charged with responsibility for ICT shall communicate the plan to staff and initiate implementation
- b) The ICT Unit shall configure a separate Virtual Local Area Network and Wi-Fi for Guest Access and temporary staff usage. In addition, the unit responsible for ICT shall ensure active technological measures are implemented to govern rule based Network Access Control and compliance.

## 3.0 BYOD PLAN REVIEW

- 3.1 At periodic intervals (once a year – recommended), the officer charged with responsibility for ICT shall review the BYOD Plan to assess whether it continues to meet its purpose and report on the same to Senior Management
- 3.2 Senior Management shall recommend for approval any changes where deemed necessary.

**TITLE: ICT PROJECT MANAGEMENT**

Doc ID: ICTP/09

Policy: All ICT projects shall follow the National Information Technology Project Management Methodology.

Purpose: To ensure that ICT projects are clearly defined, well structured, efficiently and effectively managed, and produce the desired results on time and within budget.

Scope: This procedure applies to all ICT projects within Mbarara District Local Government

Responsibility:

- a) The Project Manager is responsible for ensuring that projects run smoothly, remain on schedule, and are completed on time.

Definition:

- a) Project Manager: A project manager is the officer designated by the Chief Administrative Officer with responsibility for leading the District's ICT project from its inception to execution.

PROCEDURES:

## 1.0 ICT PROJECT SETUP

1.1 The Project Manager should use the following tools:

- Industry standards and best-practices
- A standard development method
- Project scheduling software (for estimating timelines)
- A development database for storing all information about the project

## 2.0 ICT PROJECT SCHEDULE

2.1 The Project Manager shall create the ICT Project schedule which shall indicate estimated duration and expected begin and end dates for each of the project tasks

2.2 The Project Manager shall enter the original project schedule into the ICT Project Development Database so that at the end of the project, it can be evaluated in relation to the actual times spent on the project.

## 3.0 ICT PROJECT CYCLE MANAGEMENT

3.1 Throughout the course of the project, the Project Manager shall:

- a) Continually monitor progress on each major task
- b) Document the project status at regular periodic intervals using an ICT Status Project Report.

## 4.0 ICT PROJECT MANAGEMENT POLICY REVIEW

4.1 After a project task is completed, the Project Manager shall review the project to ensure it met its objectives.

**TITLE: DATA PROTECTION AND PRIVACY**

Doc ID: ICTP/10

Policy: Mbarara District Local Government shall ensure that all personal data is processed with due care and consideration for its confidentiality and integrity in compliance with the Data Protection and Privacy Act, 2019

Purpose: To communicate specific procedures and control measures for the secure collection and processing of personal data in Mbarara District Local Government

Scope: This procedure applies to all services and functions that include the collection and processing of personal data in both electronic and non-electronic formats

Responsibilities:

- a) As required of Section Six of the Data Protection and Privacy Act (2019), the Chief Administrative Officer shall designate an officer as the data protection officer responsible for ensuring compliance with the Law within the District. All District projects including donor funded projects that deal with personal data must comply with the Law.
- b) The designated data protection officer shall take lead in coordinating the development and enforcement of the Data Protection and Privacy Program for Mbarara District Local Government
- c) Senior Management is responsible for the review of the Mbarara District Local Government Data Protection and Privacy Program and recommending to the Chief Administrative Officer for on-ward submission to Executive for approval
- d) All employees are responsible for adhering to the District's Data Protection and



## Privacy Program

### Definition:

- a) Personal data: information about a person from which the person can be identified, that is recorded in any form and includes data that relates to:
- The nationality, age or marital status of the person;
  - The educational level, or occupation of the person;
  - An identification number, symbol or other particulars assigned to a person
  - Identity data; or
  - Other information which is in the possession of, or is likely to come into the possession of Mbarara District Local Government and includes an expression of opinion about the individual.

### PROCEDURE:

#### 1.0 DATA PROTECTION AND PRIVACY PLAN DEVELOPMENT

1.1 The designated data protection officer shall in coordination with all departments undertake the following:

- i. Initiate the identification of any personal data that is collected and its purpose
- ii. use the information obtained in the section above to coordinate the implementation of Privacy Impact Assessment and develop the appropriate controls (technical, administrative and managerial)
- iii. Utilize the above information obtained above to develop the District's Data Protection and Privacy Program and submit the same to Senior Management for review. In addition, the plan should take into consideration the following globally recognized principles of data protection:
  - Accountability

- Lawfulness and fairness
- Data minimization
- Retention
- Quality and accuracy
- Transparency

1.2 Senior Management shall recommend the reviewed District's Data Protection and Privacy Program to the Chief Administrative Officer for Approval.

## 2.0 DATA PROTECTION AND PRIVACY PLAN IMPLEMENTATION

2.1 Upon approval, the designated data protection and privacy officer shall inform all departments and initiate implementation

2.2 The Officer shall maintain an updated status of implementation

## 3.0 DATA PROTECTION AND PRIVACY PLAN REVIEW

3.1 At annual intervals, the designated data protection and privacy officer shall report status findings and observations to the Senior Management for review and possible make change recommendations

3.2 The Data Protection and Privacy Program shall be subjected to a periodic audit (at least once a year), to verify that the Program and procedures are clear and actionable and continues to meet the requirements of the Law.

**TITLE: POLICY MANAGEMENT FRAMEWORK**

Doc ID: ICTP/11

**1.0 RESPONSIBILITY MATRIX**

- a) The District Council: Approve the ICT Policy Manual
- b) The District Executive Committee: Recommend the ICT Policy to council for approval
- c) The Chief Administrative Officer: Submit the ICT Policy Manual to the District Executive Committee for recommendation
- d) Senior Management: Review and submit the ICT Policy Manual to the Chief Administrative Officer for on-ward submission to District Executive Committee.
- e) Senior Management: provides top executive support for the implementation of the ICT Policy after its approval.
- f) The Officer charged with responsibility for ICT: Provide supervisory oversight for the implementation of the ICT Policy Manual and ensures that the appropriate allocation of resources are made.
- g) Unit responsible for ICT: Implement the ICT Policy Manual
- h) All Employees: Ensure compliance to the ICT Policy Manual.

**2.0 PLANNING**

2.1 The ICT Policy Manual shall be reviewed and updated at least annually or when a major organization change occurs.

**3.0 REPORTING**

**3.1 General**

Senior Management shall review proposed changes to the ICT Policy Manual on an annual basis or as per business need. This review shall include assessing opportunities for improvement and the need for changes to the ICT policy Manual with the following inputs at the minimum:

- Results of audits
- Business Process Re-engineering reports
- Follow up actions from previous reviews
- Changes that could affect ICT Policy Manual
- Recommendations for improvement

3.2 The officer charged with responsibility for ICT is responsible for providing and coordinating the ICT Policy progress reports and feedback on implementation

### 3.3 Review Output

Records shall include the output from the Senior Management review and any decisions and actions related to the improvement of the ICT Policy Manual and Resource requirements.

## 4.0 RESOURCE MANAGEMENT

4.1 Provision of resources: During planning and budgeting processes and as needed throughout each financial year, Senior Management shall determine and ensure that the appropriate resources (people, equipment, facilities and funding) are available to implement and maintain the ICT Policy and continually improve its effectiveness.