# COUNTY GOVERNMENT OF MERU ICT POLICY DRAFT

## Table of Contents

1. **OBJECTIVE OF THE ICT POLICY** ........................................................................................................ 2
2. **SCOPE** .............................................................................................................................................. 2
3. **ICT STANDARDS POLICY** .................................................................................................................. 2
4. **NETWORK DEVELOPMENT POLICY** .................................................................................................. 2
5. **NETWORK ACCESS, SECURITY AND MANAGEMENT POLICY** ....................................................... 3
6. **INVENTORY AND IO REPORT** ............................................................................................................ 3
7. **INTERNET POLICY** .......................................................................................................................... 3
8. **SYSTEMS AND PASSWORD POLICY** .................................................................................................. 4
9. **EMAIL USE AND WEBSITE POLICY** ............................................................................................... 4
10. **USER SUPPORT, TECHNICAL ASSISTANCE AND COMPLAINT POLICY** ...................................... 4
11. **POLICY ON PRINTERS, TELEPHONE LINES, FAX AND COPIERS.** ............................................. 5
12. **DATA CENTRE ACCESS POLICY** ....................................................................................................... 5
13. **BACK UP AND DISASTER RECOVERY POLICY** .............................................................................. 5
14. **ICT TRAINING POLICY** .................................................................................................................. 5
15. **PROCUREMENT POLICY** .................................................................................................................. 6
16. **STATEMENT OF ENFORCEMENT OF POLICY** .............................................................................. 6
1. OBJECTIVE OF THE ICT POLICY
   - To standardize and enhance ICT infrastructure, equipment and systems.
   - To ensure provision of secure, adequate and reliable information systems and their operational environment.
   - Provide guidelines on the usage of ICT software, hardware, custom systems, cloud and shared services.
   - To promote confidentiality, integrity and availability of county information and information systems.
   - To harmonize and coordinate ICT automation and expansion initiatives.
   - To ensure application of best practices and standards in provisioning and automation.
   - To maximize use of IT resources and ensure maximum return on investment.
   - To leverage on the IT resources to bring about a knowledge-based workforce.
   - To prevent misuse of information, information systems and avoid abuse of IT privileges.
   - To create, retain and safeguard proprietary rights of our ICT resources.

2. SCOPE
   This policy entails guidelines to accessing, implementing, developing or using County Government of Meru ICT based Information and all the ICT resources that it owns, manages, supports or operates.

   It relates to all the Information technology resources, services and facilities computers (Laptops and desktops), iPad, internet, telephone system, printers and copiers, operating systems, servers, software, databases, wireless communication, email systems and ERP.

   All employees, business partners and the volunteers are supposed to adhere with the policy.

   The policy includes the following:

3. ICT STANDARDS
   The county government of Meru ICT standards guided by ICTA and PPOA guidelines takes precedence. These standards shall be updated time to time as ICT environment changes or as ICTA and PPOA standards change.

4. INFORMATION AND DATA
   The county shall endeavour to protect all data before, during and after transmission through the ICT systems. The county shall as well develop information classification policy to protect its information.

5. NETWORK DEVELOPMENT
   County Government of Meru will develop and support wide and local area network as a basic infrastructure service for the facilitation of sharing electronic information and resources by the members of county government and the public.

   The county network should be;
   a) Universally available: the network will be designed and implemented in such a way as to serve all government departments.
   b) Reliable; High levels of availability, reliability and maintenance will be major objectives in the construction and operation of the ICT network infrastructure.

   The design and construction of the county network infrastructure will take into account emerging technologies and standards wherever possible.
ICT Infrastructure Development

i. Development plan; ICT shall prepare a rolling five (5) year infrastructure architecture and plan, advising on appropriate developments aimed at ensuring the adequacy of the ICT infrastructure in future. This plan will take account of the county government of MERU strategic plan; usage and demand patterns; technological change; security; management and cost implications.

ii. Implementation of new developments
Prior to installation of the “live” situation, major network developments shall be “soak-tested” in offline simulation. For up to two months after the live installation of the new development, the network provision that it is to be replaced shall, wherever possible, remain in place as a “fall-back” in the event of any subsequent failure of the new development when it is subject to actual user demand.

iii. ICT network provision in new and refurbished buildings
Network provision for new and refurbished buildings shall be made in accordance with the specification published from time-to-time by the ICT directorate. All new buildings to be erected for County Government of Meru shall incorporate an appropriate structured data wiring system to allow connection to the county network infrastructure based on ICT certified standards.

6. NETWORK ACCESS, SECURITY AND MANAGEMENT

i. ICT shall develop a comprehensive security policy to protect, govern and build resilience before, during and after attacks.

ii. The ICT reserve the right to assign access to the networks.

iii. Firewalls and Intrusion Detection systems shall be used across the entire County Government of Meru network to monitor and prevent hackers, viruses and worms including all other forms of attacks.

iv. The in-charge of network shall ensure that this policy is adhered to. Failure to do this may necessitate disciplinary action depending on circumstances.

v. All computers hooked into the network shall mandatorily have an up-to-date antivirus software to prevent viruses and all other forms of malicious code.

vi. All staff are also expected to seek authority from ICT support before hooking any laptop to the network. ICT shall define filter levels for all sections of the network.

vii. Staff are also expected to timely report outdated versions of antivirus for action to ICT support.

viii. All servers shall likewise have antivirus and a form of monitoring to ensure that only authorised users have access.

ix. The Network Manager, shall monitor and document ICT network performance and usage and shall maintain regular monthly reports.

7. INVENTORY AND IO REPORT
ICT shall develop, maintain and update an inventory report including user Input Output report. This will be base resource needs guide.

8. INTERNET
All authorized users have right to internet access. Access to internet is restricted to appropriate content.
Online privacy and security shall not be guaranteed but all measures shall be undertaken to reduce, manage and stop related incidents.

9. SYSTEMS AND PASSWORD POLICY
   i. Passwords are private and prove of right to use or having used a protected service.
   ii. Good password complexity is recommended and should be a combination of alphanumeric and special characters (l_?$^*#), i.e. complex, but easy to remember.
   iii. Passwords must be at least six (6) characters.
   iv. Users are required to change their passwords at least every three months.
   v. Passwords shall lock for every three unsuccessful attempts.
   vi. The maximum number of sessions per user shall be three (3).
   vii. Password Management, shall be the responsibility of Systems Administrator
   viii. A user whose password has expired, or account locked shall (upon request through IT support) be assigned an initial password by the systems administrator. The affected user must change the initial password immediately for security reasons; bearing in mind that users are solely responsible for actions committed using their own accounts.

10. EMAIL USE AND WEBSITE
    i. The e-mails shall be provided for to all staff on prefix firstname.middlename@meru.go.ke.
    ii. It is the policy of County Government of Meru to have e-mail (from and to county recognized domains) recognized as official means of communication. Thus an email is an official document.
    iii. The website shall be updated frequently on current issues happening within the organization with respective departments expected to forward information to the Communication department for vetting before uploading the information to the website.
    iv. There shall be a framework that allows respective departments to manage own content on the website.
    v. Hosting and website development shall be based on an ICT certified requirements document.

11. USER SUPPORT, TECHNICAL ASSISTANCE AND SERVICE DELIVERY
    All user requests for assistance shall be properly logged using support helpdesk system.
    i. ICT officers will be available to offer technical support on any software or hardware needs.
    ii. Officers’ assigned equipment must ensure they are not exposed to risks that can cause their damage.
    iii. All ICT technical assistance requests shall be channelled through the centralised helpdesk system. Requests and/or complaints made through other means e.g. telephone shall be given less priority than requests made through the helpdesk system.
iv. Provision of a global support e-mail which allows all ICT personnel to receive the issues raised by ICT helpdesk@meru.go.ke shall be used.

v. Dedicated telephone numbers and extensions shall be used for the helpdesk.

vi. Where applicable, equipment to be used out of office shall be accompanied by an ICT Technician to ensure proper packaging, offloading and installation at destination.

vii. All ICT equipment shall be maintained in accordance with the procedure for ICT equipment maintenance.

viii. In areas where the directorate has no adequate internal capacity, maintenance contracts shall be entered into with service providers.

ix. The directorate shall deliver its services based on the service charter.

12. POLICY ON PRINTERS, TELEPHONE LINES, FAX AND COPIERS.
Staff are expected to use them responsibly. Irresponsible/excessive use of the above for personal purposes is discouraged. Emphasis is laid on shared printing points with user document protection. A password or PIN to print, photocopy or scan must be provided. User statistics must be maintained.

13. DATA CENTRE ACCESS POLICY
Only authorised ICT personnel are allowed to access the ICT data centre and DRC. All other persons must be accompanied by authorised staff and must sign a visitor’s book. The head of ICT reserves right to authorize such personnel and visitors.

14. BACK UP AND DISASTER RECOVERY POLICY

Backup Inventory
An inventory of critical applications backup media and supporting materials must be maintained. A copy of the inventory must be securely stored off site or in a fireproof container at the facility that hosts the application. It is recommended that an inventory of backup media and materials is recommended for all other information resources.

End User Backup
Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is strongly encouraged that end users save their data.

System Backup
All system backup shall be the responsibility of the system owner. ICT will set up backup systems in collaboration with users.

15. ICT TRAINING POLICY
Every section within ICT department shall identify training needs every beginning of financial year and forward to the ICT divisional committee. The ICT divisional committee shall analyse the trainings relevant for every section to make sure that the training requirements are relevant to the various sections staff and within budget and forward the names and requirements to the manager in charge of ICT. The Director ICT shall, upon his approval, forward the training requirements to Human Resource and Administration for implementation.
16. PROCUREMENT POLICY

Procurement of ICT and ICT related equipment should comply with stipulated ICT standards and processes.

17. STATEMENT OF ENFORCEMENT OF POLICY.

i. The Director/Head of ICT, in liaison with ICT Governance Committee, shall be responsible for enforcing these policies.

ii. The Head of ICT shall monitor the implementation of this policy.

iii. This policy shall guide all IT undertakings, usage and all related issues in all forms in the county.

iv. Violation of this policy shall be addressed by appropriate county and national legal mechanisms.
# ICT STANDARDS POLICY

## Table of Contents

1. **INTRODUCTION** ..................................................................................................................................... 9
   1.1. Background ................................................................................................................................... 9
   1.2. Rationale and situation analysis ................................................................................................. 10
   1.3. Stakeholders’ analysis summary ................................................................................................. 10
2. **Standard and Guidelines Statement** ................................................................................................... 12
3. **Authority** ............................................................................................................................................. 12
4. **ICT MISSION AND VISION** .................................................................................................................... 12
5. **OBJECTIVE OF THE STANDARDS** ........................................................................................................ 13
   a. Specific objectives ....................................................................................................................... 13
   b. Key Principles .............................................................................................................................. 13
6. **ICT GOVERNANCE** ............................................................................................................................... 13
   1.2. Technical Committees................................................................................................................. 14
7. **ICT INFRASTRUCTURE STANDARDS AND GUIDELINES** .................................................................. 14
   7.1. General IT Equipment Guidelines ............................................................................................... 15
   7.2. ICT equipment management guidelines ..................................................................................... 15
   7.2.1. Roles and Responsibilities ................................................................................................... 15
   7.3. Procurement ..................................................................................................................................... 16
   7.3.1. Technical Specification Principles ....................................................................................... 17
   7.3.2. Evaluation............................................................................................................................ 17
   7.3.3. Inspection ............................................................................................................................ 18
   7.3.4. Certification ......................................................................................................................... 18
   7.4. Inventory ..................................................................................................................................... 18
   7.5. Installation and Operation of ICT Equipment ............................................................................. 19
   7.5.1. General Installation and Operation Guidelines .................................................................. 19
   7.5.2. Administration .................................................................................................................... 19
   7.5.3. Change management guidelines ......................................................................................... 20
   7.5.4. Prohibition........................................................................................................................... 20
   7.5.5. ICT Equipment Assessment and Audits ......................................................................... 20
   7.5.6. Maintenance ......................................................................................................................... 20
   7.5.7. Decommissioning and Disposal Guidelines ......................................................................... 21
   7.5.8. Disposal Mechanisms.......................................................................................................... 22
8. **SOFTWARE STANDARDS AND GUIDELINES** ......................................................................................... 24
8.1. ACQUISITION OF APPLICATION SOFTWARE................................................................. 25
  8.1.1. Application Software......................................................................................... 25

8.2. SYSTEM SOFTWARE SPECIFICATION................................................................. 27
  a. Systems Software..................................................................................................... 27
  b. Application Development Software........................................................................ 27

8.3. SOFTWARE ACQUISITION..................................................................................... 28
  a. Customized Commercial Software (COTS)............................................................ 28
  b. Open Source Software............................................................................................. 30
  c. Application software............................................................................................... 30

8.4. SOFTWARE DEVELOPMENT................................................................................ 31
  a. System Development Process................................................................................ 31
  b. Software Development Lifecycle.......................................................................... 32
  c. Procurement.......................................................................................................... 32
  d. Maintenance.......................................................................................................... 33
  e. Disposal................................................................................................................. 34

8.5. Prohibited Software............................................................................................. 34

8.6. Software copyright compliance............................................................................. 35

8.7. Software Audits.................................................................................................... 35

8.8. Training and Knowledge Transfer....................................................................... 35

8.9. Software Custody.................................................................................................. 35

8.10. Licenses............................................................................................................... 35
1. INTRODUCTION

1.1. Background

The County Government of Meru (CGM) vision is *A United Prosperous Green Model County*. Thus our mission is to facilitate sustainable development and wealth creation in the County through e-commerce, technological innovations and industrialization that leverages on our skilled human resources, agriculture, wildlife, bio-diversity and cultural heritage. In so doing the Governor shall lead the county in upholding values of *Integrity, Team work, Inclusiveness, Innovativeness, Hard work, Transparency and Accountability*. To achieve the said vision the County has prioritized key sectors including Governance and Public Administration; *Information and Communication Technology (ICT)*; Justice, Cohesion and Security for Development; Disaster Preparedness and Management; Planning; Health; Social Protection, Culture and Recreation; Infrastructure; Financial Services, Trade, Co-Operatives and Enterprise Development; Industrialization; Land; Agriculture; and Tourism. These have been identified as key to moving all aspects of our county forward.

The Constitution of Kenya, 2010 in Article 35 (1) (a) guarantees that every citizen has the right of access to information held by the State; and information held by another person and required for the exercise or protection of any right or fundamental freedom and that every person has the right to the correction or deletion of untrue or misleading information that affects the person.

The article further goes to state that the State shall publish and publicize any important information affecting the nation.

The County ICT Strategy further identifies specific tenets of information systems that focus on areas that need to be strengthened to enable response to this constitutional requirement. The County’s Integrated Development Plan (CIDP) 2013 - 2017 clearly identifies ICT as a catalyst to attaining efficiency in multiple facets of the above areas.

As the county moves towards the adoption of ICT technologies, there is therefore need to have a basis for standardization to ensure that ICT implementations occur in a coordinated approach with reference to common set of standards and guidelines. Lack of standards will present challenges in integration of systems across various sectors.
Therefore as ICT directorate in the County and other departments increasingly embrace ICT in service delivery, it is therefore necessary to have a common approach based on recognized best practices and standards.

1.2. Rationale and situation analysis
ICT capacity in the public sector has grown as demonstrated by implementation of various systems in the country such as GHRIS, IFMIS, IPPD, LAIFOMS and other systems. ICT infrastructure is being heavily funded as witnessed by the numerous undersea cables and the NOFBI project to connect the entire country to a national fibre optic network.

The CGM has improved ICT through the installation of backbone connectivity at the County headquarters and Sub County public offices. The plan is to have all county offices connected and service delivered in real-time to the public. CGM has heavily invested in provision of ICT tools such as systems, tablets, computers, printers and other required items, have led to improved service delivery and enhanced information exchange within the country.

The challenge in most ICT powered environments is ensuring consistency in ICT implementation, security, sustainability and harmonization of resources. The department has developed a roadmap that guides service delivery, public/customer satisfaction, security and privacy. The challenges experienced by ICT service areas include low level of capacity in terms of technology, centralization of the ICT resources at the national level, lack of information systems integration and ICT service sharing.

The objective of these ICT standards and guidelines is to ensure consistency in ICT initiatives and management so as to achieve standardization and create efficiency and improve service delivery.

1.3. Stakeholders’ analysis summary

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>ICT Sector Expectations of the Stakeholders</th>
<th>Stakeholder Expectations from ICT Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizens</td>
<td>Active participation</td>
<td>Timely and accurate information</td>
</tr>
</tbody>
</table>
<pre><code>                                    | Cooperation                               | Effective and                            |
</code></pre>
<table>
<thead>
<tr>
<th>Other Departments</th>
<th>Cooperation and support</th>
<th>Automation of the processes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clear definition of the need</td>
<td>Appropriate Training</td>
</tr>
<tr>
<td>Media</td>
<td>Awareness Support</td>
<td>Access to information</td>
</tr>
<tr>
<td>Central Government</td>
<td>Financial Support Accessibility of the Central Systems Licensing of the media channels</td>
<td>Implementation of the systems Setting of standards and guidelines</td>
</tr>
<tr>
<td>Global partners</td>
<td>Accessibility of information on products and services</td>
<td>Markets, Visibility and Financing</td>
</tr>
</tbody>
</table>
2. **Standard and Guidelines Statement**

The County Government of Meru will continuously enhance its organizational capacity by adopting modern technologies, skills development and innovation to develop systems that are responsive to the needs of its residents. These standards will provide guidance across the county to ensure that ICT resources are optimally utilized in order to achieve efficiency in service delivery.

The standards promote principles that guide implementation of robust ICT infrastructure, Information systems, support services and operational capacity.

3. **Authority**

The standards and guidelines derive the authority from:

(i) The Constitution of Kenya;
(ii) Kenya Communications Act 2009;
(iii) The National ICT Policy, and
(iv) any other relevant legal provision and Government policies that may come into force after initial implementation of these standards and guidelines

4. **ICT MISSION AND VISION**

**Vision**

An empowered and knowledgeable County

**Mission**

Provision of a robust IT and Communications platforms for efficient service delivery and visibility.

**Sector Objectives**

- Use technology to create awareness, inform and educate the Citizens on the relevant development issues and activities of the County Government.
- To provide data and information to other sectors for better planning
- To enhance operations of the county government and reduce operational costs by automating county internal services and processes
- To provide a robust platform for quality technology driven service delivery and to create a virtual supermarket for products and services available and offered in the County
5. OBJECTIVE OF THE STANDARDS

5.1.1. Specific objectives

i) Aligning county government of Meru ICT standards with national and world standards (ICTA and CRA regulations)

ii) Support the development, implementation and maintenance of ICT Systems in County;

iii) Enhance information security of County ICT systems.

iv) Promote efficient and effective operations and usage of ICT systems within the County;

v) Encourage and support innovations in technology development that contribute towards job and wealth creation;

vi) Facilitate efficient and economic use of resources to ensure that technology does not become an expensive venture to the County;

vii) Facilitate the development of ICT skills to support ICT systems in the County;

viii) Promote efficient communication among the County staff and stakeholders;

ix) Promote information sharing, transparency and accountability within County and towards the general public and other stakeholders.

5.1.2. Key Principles

This standard shall be guided by the following key principles:

(i) Mainstreaming of ICT in the County
(ii) Integration of ICT systems
(iii) Adherence to best practices & policies
(iv) User and customer satisfaction

6. ICT GOVERNANCE

1.1. Governance Committee
There shall be a committee composed of The CEC Member in charge of ICT as the Chair or a
designated representative. Other members will be Chief Officers of various departments, the
Director ICT and ICT technical representatives. The Director ICT shall be the secretary of the
committee.

The ICT Governance Committee shall formulate and advance the programs of the ICT
Directorate within the county. The committee will give direction for County ICT programs

The roles of the ICT Governance Committee shall include but not limited to:

- Review and provide advice on ICT investment priorities in the county;
- Mobilization of resources for ICT investment in the county;
- Provide ICT strategies, policies and standards;
- Provide guidelines and policies for technical ICT programs
- Provide general advice and guidance on ICT matters in the county;
- Raise awareness on the strategic value of ICT in the county; and
- Promote information sharing on ICT programs in the county

1.2. Technical Committees

There shall be a technical committee chaired by the Director ICT, representative from all ICT
sections such as Network management, system administration, software development, web
and online management and customer service. This committee will deal with matters of
innovation, technical advice, disposal/decommissioning, strategy, inspection and certification
of ICT Systems, among others and in line with the existing laws and regulations.

Where cross-cutting issues of ICT are involved such as evaluation, the Director - ICT will
appoint representatives as appropriate.

7. ICT INFRASTRUCTURE STANDARDS AND GUIDELINES

The ICT Standards and Guidelines recognize that ICT comprises both equipment and the
systems. The following section specifies IT equipment standards and guidelines.
The ICT equipment standards and guidelines stipulated herein shall apply and be used in the procurement, management, maintenance and disposal of all ICT equipment.

7.1. General IT Equipment Guidelines
The following guidelines shall be observed by the County Government of Meru:

a) County computing environment shall endeavour to be technology-neutral driven by service requirements.
b) Information technology shall aim at improving service delivery, improve public awareness and create knowledge base.
c) IT service delivery shall leverage current and new technologies.
d) Guidelines on relevant ICT infrastructure, software, and applications shall be developed and reviewed from time to time for adoption and implementation.
e) New technologies, products or services shall take cognisance of existing infrastructure, platform and prevailing guidelines.
f) Advances in technology, services and embedded applications shall be identified, adopted and implemented where possible.

7.2. ICT equipment management guidelines
These guidelines shall direct the County Government of Meru in the use and management of all ICT equipment not limited to personal computers, desktops, workstations, laptops, mobile devices, printers and peripheral devices. This also includes telecommunications equipment such as routers, switches, hubs and other network devices.

The ICT equipment management guidelines aim to:

a) Guide procurement and disposal of ICT equipment
b) Ensure the County Government receives value for money on ICT equipment
c) Ensure compatibility and interoperability both within and across County.
d) Ease maintenance
e) Ensure cost effective use of ICT equipment.
f) Ensure consistency in ICT equipment performance
g) Maximize the equipment functionality
h) Improve end-user performance and experience

7.2.1. Roles and Responsibilities
The ICT Directorate shall develop and update minimum specifications of all categories of ICT equipment on a regular basis. Specification of ICT equipment aims to ensure that appropriate equipment is acquired that is fit for purpose, cost effective, and has extended useful life.

The ICT Directorate shall be charged with the responsibility of installation, upgrading, supporting, maintaining and inventorying all ICT resources.

The Chief Officer – lands, ICT and Planning shall enforce these standard specifications and give advice where specifications above the minimum are required.

While developing specifications, the ICT Directorate shall take into consideration the end user requirements.

The Supply Chain Management unit shall liaise with the ICT Directorate to procure quality ICT equipment and consumables in a timely manner.

End-users shall take care of any ICT equipment allocated to them. Any issues arising in the course of usage of the equipment shall be brought to the attention of the ICT Directorate.

The ICT Directorate shall also sensitize end-users on the proper usage of equipment in their custody.

7.3. Procurement

Procurement of IT hardware, software and 3rd party services shall conform to Public Procurement & Disposal Act and relevant Government circulars. ICT directorate shall ensure that end user equipment procurement is done with the guidance of the ICT function and knowledge of the heads of user department.

Procurement of ICT equipment shall be channelled through the Head of ICT who shall be responsible for the approval of all technical specifications for the equipment, as well as ensuring that the guidelines stipulated herein are adhered to.

Due diligence shall be undertaken by ICT directorate before taking the decision to acquire ICT resources. Such resources must be deemed necessary, relevant and cost effective by the department in consultation with requisitioning department. To the greatest extent possible the ICT Directorate shall ensure that ICT cost and ICT footprint is kept to a minimum.

The ICT Directorate shall endeavour to consult and share information with other departments and agencies for continuous improvement in the ICT equipment specification process.
7.3.1. Technical Specification Principles

When developing specifications, the following equipment considerations shall be made:

a) **Total lifecycle:** These specifications are meant to ensure that equipment acquired have useful life of not less than five years.

b) **Functionality:** This intends to guarantee that operational requirements intended to be performed by ICT equipment can be achieved effectively and efficiently with the equipment specified.

c) **Security:** This addresses the need to protect system data and equipment, and the operational environment from loss or compromise.

d) **Interoperability:** This seeks to facilitate the exchange of information between potentially heterogeneous systems through conformance to open standards.

e) **Compatibility:** This addresses the ability of ICT equipment components to effectively and efficiently work together in an integrated system.

f) **Scalability:** This is intended to ensure that the acceptable ICT components enhance the ability of the equipment to support future growth and increased throughput.

h) **Accessibility:** This addresses operational readiness that includes the ability of users and operators to access the equipment in a timely fashion, to perform its intended functions.

i) **Long-term support:** This addresses the availability of vendor and/or internal support, including parts and labour.

j) **Upgradability:** ICT component installations that need updates shall be updated according to the latest official versions available.

The ICT Directorate shall use requisition and acceptance forms to ensure that requests for procurement of ICT equipment are approved by the respective Chief Officers.

7.3.2. Evaluation

The Procurement office should ensure that the ICT Directorate is involved in the technical evaluation and inspection process of ICT

Technical evaluations shall ensure that the equipment is fit for the purpose intended and that it meets the required specifications.
ICT Directorate shall ensure that warranty agreements and guarantees are provided and also oversee administration of the same. The minimum warranty for all ICT equipment shall be one year, and three years for servers. All warranties shall be in writing.

The ICT Directorate or a member appointed by the Chief Officer shall be involved in the technical evaluation and inspection processes.

### 7.3.3. Inspection

The ICT Directorate shall develop guide to aid inspection process as per the relevant procurement law.

Upon delivery of the equipment, the ICT Directorate shall work with the relevant inspection committee to inspect and ascertain that they meet or exceed the specifications as requisitioned.

The Department shall work in conjunction with the relevant inspection and acceptance committee to validate the receipt of all ICT equipment procured or donated to the County.

All acquisitions and donations shall be required to meet the minimum specifications.

### 7.3.4. Certification

The ICT Directorate shall certify all received equipment and systems upon being involved in evaluation and inspection.

This forms the basis of paying for the system.

### 7.4. Inventory

a. All equipment received through purchase or donation by the County shall remain the property of County and must be electronically tagged appropriately.

b. The ICT shall maintain an electronic inventory of all ICT equipment for the County Government.

c. All equipment and assets whether new, transferred and/or written-off shall be recorded by the ICT Directorate for audit and other asset management purposes.

d. The inventory of ICT assets shall indicate product details (product number, serial number, part number, etc.), tracking information, maintenance schedules and warranty information.
e. The ICT shall ensure that ICT component is captured in the clearance certificate for all officers exiting the county.

f. Officers exiting the County shall be required to surrender all ICT equipment in their custody to the ICT Directorate.

7.5. Installation and Operation of ICT Equipment

Installation of ICT equipment includes but is not limited to equipment upgrades, part replacements, assembly, and part transfers, among others.

7.5.1. General Installation and Operation Guidelines

a) The hardware installation shall have sufficient capacity to serve the County
b) The ICT equipment shall work as designed
c) The hardware shall work well and without failure
d) Before installation, the equipment must be tested to ensure they work as required.
e) The equipment shall be used for the intended purpose.
f) Associated licensing for the equipment need to be validated.
g) Only qualified personnel shall be allowed to install the ICT equipment
h) The installation of ICT equipment shall adhere to the OEM instructions.
i) Only trained and qualified personnel will be allowed to operate the ICT equipment
j) ICT equipment shall be operated within recommended environmental conditions of temperature, humidity, etc.
k) Access and maintenance of equipment shall only be carried by authorised and accredited personnel.

7.5.2. Administration

The ICT Directorate will be responsible for administering ICT infrastructure, including ICT equipment.

Specific authority shall be obtained from the relevant section head before installation and operation on ICT equipment can be undertaken.

Installations that will affect mission critical equipment shall require prior notifications to equipment administrators and users of the anticipated downtime.
Where equipment has to be moved, a document to track movements of hardware shall be used.

End-users are prohibited from carrying out any installation, maintenance or upgrade of whatever nature.

### 7.5.3. Change management guidelines

Change management of ICT equipment shall be guided by the following considerations:

- **a)** Define nature of installation or operation
- **b)** Reason for the change
- **c)** Specification of client services affected
- **d)** Any prerequisites and fall back plan
- **e)** Who is involved in the installation/operation
- **f)** Required time and resources for the installation
- **g)** Details of the change instituted

### 7.5.4. Prohibition

ICT equipment that do not meet industry and safety standards is prohibited from being deployed.

### 7.5.5. ICT Equipment Assessment and Audits

The ICT Directorate will periodically conduct assessment/audit of County Government ICT equipment to ensure compliance with performance standards and requirements, and ensure equipment component parts are as indicated in the inventory.

### 7.5.6. Maintenance

ICT equipment maintenance may be done in-house by ICT Directorate where a maintenance function shall be established. The department shall develop a schedule of maintenance for equipment as well as an equipment upgrade plan.

Sub-contracting for maintenance shall be through appropriate justification and approval by the Accounting Officer in consultation with the ICT Directorate. Due diligence shall be undertaken in engaging and retaining such contractors.
The ICT directorate shall prepare an annual maintenance report and forward it to the respective Chief Officer.

ICT Directorates shall undertake surveys to identify obsolete equipment for the purposes of disposal. Where such equipment contains data, that data shall be permanently erased using suitable mechanisms.

ICT Directorate shall electronically track the physical locations and status of all equipment where possible.

The ICT Directorate shall draw up a maintenance schedule of all equipment under its custody. The schedule shall specify the frequency levels and type of maintenance for each type of equipment.

In case of mission-critical equipment, users shall be notified of the maintenance in advance.

The ICT Directorate shall ensure that the vendor’s SLAs terms are made to the satisfaction of County.

ICT equipment maintenance shall consider routine/preventive, upgrade, and repair maintenance as may be required.

7.5.7. Decommissioning and Disposal Guidelines

Decommissioning is the formal termination of equipment and its removal from the IS operating environment. The ICT Directorate may decommission equipment that is no longer needed on its Information System.

Equipment may be decommissioned if it meets one or more of the following criteria:

a) Redundant equipment
b) Change in IS architecture
c) Technologically obsolete equipment Insufficient capacity to handle application and/or user requirements
d) Where upgradability options have been exhausted
e) Where equipment has become unsafe

Decommissioning of equipment will be undertaken through committee. Candidate equipment for decommissioning determined to be still useful and still meets the required safety standards may be reassigned to lesser demanding tasks or appropriate environment.
Decommissioned equipment that is no longer required shall be treated as candidate items for disposal.

County may dispose of equipment that it deems no longer useful.

Identification of the equipment for disposal shall be based on the following criteria:

a) Damaged beyond repair  
b) It cannot be upgraded  
c) If the repair cost is higher than the cost of buying a new one (cost will either exceed or is considerably close to the cost of acquiring a new replacement)  
d) If the parts and/or consumables are not available  
e) End of life and no longer supported by the OEM

Departments wishing to dispose of ICT equipment should seek advice from the ICT Directorate.

7.5.8. Disposal Mechanisms

When equipment is identified for disposal, all application software and data should be backed up and permanently erased from the equipment in accordance with the relevant regulations or guidelines. Inventory tags shall also be removed and destroyed while updating the inventory system.

Equipment identified for disposal shall be handed over to the County committee responsible for disposal to be disposed of in accordance with the relevant disposal regulations.

ICT equipment identified for disposal but deemed to be still usable may be transferred to other institutions such as schools and colleges and installed for low-end non-critical use where appropriate. Adherence to the statutes (in consultation with County Assembly Committee) and regulations on disposal must always be observed.

ICT equipment for disposal shall be tagged with the standard labelling conventions and appropriately physically secured.

The ICT Directorate shall electronically keep an inventory of all the ICT equipment that has been disposed of.
Equipment that may not be used as a whole may be disposed of by cannibalizing. Such equipment may be cannibalized for those components that may be reused. Proper records shall be kept to indicate where such components are used or stored.

The ICT Directorate may recommend the following alternative methods for disposal to the County:

a) Donation: The County shall upon authority from the Accounting Officer/Head of ICT donate identified equipment and components, to deserving Government institutions or individuals.

b) Trashing: ICT equipment that cannot be sold and have no useful components, and are not worth donating, shall be trashed. Such equipment shall be forwarded to licensed e-waste handlers for the right disposal channels.

The head of the directorate shall give advice before any ICT equipment is disposed of by the County Government.
8. SOFTWARE STANDARDS AND GUIDELINES

Information System is an integrated set of components i.e. software, hardware, and human resource for collecting, storing and processing data and for delivering information, knowledge and digital products in an organization. Software is a set of programs, procedures and algorithms that instruct the computer how to carry out specified functions. The standard provides and prescribes best practices for software development, acquisition, support and maintenance by County Government of Meru. These best practices have been recognized to significantly contribute to the successful acquisition, deployment and utilization of information systems.

Software guidelines and standards aims to assure software quality, ensure software internal usability, and help evaluate the software product. Their application by the County aims at achieving the following objectives:

i. Ensure data/ information sharing across County;

ii. Enhance user satisfaction;

iii. Ensure compatibility;

iv. Enhance unified support and management;

v. Ensure cost effectiveness;

vi. Provide a platform to support a unified Human Information System

vii. Improve staff productivity;

viii. Ensure coherence in systems upgrade management.

In addition, when deploying software the County shall ensure conformity to WHO Health Informatics Standards and software international standards including but not limited to:

i. ISO 9126- 1 on Software product quality

ii. ISO/IEC 9126-2 on External usability metrics

iii. ISO/IEC 9126-3 on Internal usability metrics

iv. ISO/IEC 9126-4 on Quality in use Metrics

v. ISO 9241-11 on Guidance on usability
vi. ISO 14598 – 1 on Software product evaluation.


The guidelines shall publish acceptable standards for software products bought off-the-shelf, Free and Open Source Software (FOSS), software developed internally or developed by contracted third parties. For the purpose of this guideline, software is classified in three broad categories based on its purpose, functionalities, type, or area of application:

1. Application software.

2. System software.

3. Application Development software.

8.1. ACQUISITION OF APPLICATION SOFTWARE

8.1.1. Application Software

Application software refers to computer software designed to perform a specific set of tasks.

Acquisition of application software, unlike other types of software shall require an elaborate approach due to the nature of its specialization. Since applications shall be acquired for a diverse business processes and support services, the procedures guiding this acquisition shall be determined by the nature of the application as well as availability in the market of off-the-shelf programs that address the specific business requirements. In all application software acquisition procedures, a technical committee comprising of business, key stakeholders and ICT subject experts should be set up. In addition, application of a standard software development methodology and project management guidelines shall be enforced.

Acquisition of application software shall therefore fall under the three broad procedures:

a. In-house Development:

All in-house development of business software shall be coordinated by the ICT Directorate. The software development process will adopt a project management approach. The ICT Directorate will constitute a development team consisting of various specializations as may be required in specific software development task. These shall include software developers with expertise in target development platform, business/systems analysts, business/systems designers, database experts, network and communication, security specialists, system testers among other skills that may be required in different project.
b. Outsourced Development:

For sophisticated system development initiatives that require skills and knowledge not available within County, an external developer may be contracted to deliver the business application. In this case, the implementing / Department within County in collaboration with ICT Directorate shall adopt a project and constitute a technical team consisting experts in the business and technical process, business/systems analyst and the relevant ICT skills. The technical team shall:

a) Develop a concept paper and seek approval from the ICT governance committee
b) Develop a Request for Proposal/Terms of Reference including well-articulated and comprehensive business and functional requirements that shall inform a contractor to enable them in the submission of proposal that delivers a turn-key business solution.
c) Evaluation of both the technical and functional requirements to ensure that they are clearly aligned to the needs of the County Government.
d) Ensure that the contracted firm delivers source codes, implementation manuals, end user manuals and all other necessary documentations.
e) Manage the entire process using the acceptable project management methodology
f) Establish and ensure conformance to the Service Level Agreement


c. Commercial off-the Shelf:

A project technical team in some cases having developed the business and functional requirements in software development process may seek to acquire a solution that is readily available in the market. Examples of such solutions include modules of ERP software. In this case, the implementing agency within County in collaboration with ICT Directorate shall constitute a technical team consisting experts in the business process, business/systems analyst and the relevant ICT skills. The technical team shall:

i. Develop a concept paper and seek approval from the ICT governance committee
ii. Develop a detailed specification of the system that comprehensively meets the business and functional requirements of the client.
iii. Review existing deployment of such systems for the purposes of benchmarking.
iv. Manage the entire process using the acceptable project management methodology
v. Ensure proper knowledge transfer to the client for sustainability of the system
vi. Ensure that the contracted firm delivers implementation manuals technical manuals, end user manuals, licenses and all other necessary documentations.

vii. Ensure there is a contract document on post implementation that includes Service Level Agreement, warranties, Support and Maintenance for a minimum of two years

8.2. SYSTEM SOFTWARE SPECIFICATION

a. Systems Software

System software refers to computer programs used to start and run computer systems and networks, including but not limited to Operating Systems.

County shall endeavor to upgrade, to the minimum requirements, all software that fall below the recommended standards. The County Government shall ensure that:

i. Licenses for commercial operating system are provided upon acquisition, duly registered and subsequently renewed as per the requirements of the copyrights;

ii. The latest stable version is purchased in each case;

iii. Vendor support is provided;

iv. The software is regularly updated with the latest patches.

v. Shall ensure that only licensed system software is used

ICT Directorates shall keep an inventory of all operating system software installed and closely monitor and evaluate to ensure licensing and copyright agreements are maintained. The head of the shall take custody of all operating system software installation materials, including manuals and related materials where supplied. They shall also ensure that where possible, back-ups are carried out before any reinstallation or upgrade of an operating system. The s shall organize training for users on any new client operating system software.

b. Application Development Software

Application development tools are used to translate and combine computer program source code and libraries into executable programs i.e. compilers and linkers.
The County Government shall ensure that ICT officers responsible for development of software are adequately trained on all application software acquired.

The ICT Directorate shall take into consideration the following when acquiring application development software:

a) Type of application to be developed; Desktop application, Web based application or server application and mobile application.

b) Operating System platform the software to run on.

c) Integration with the existing development tools.

d) Database to be used by the application.

e) Compatibility with existing and future hardware and software platforms.

f) Assistance in enforcement of coding Standards

g) That has community support base

8.3. SOFTWARE ACQUISITION

a. Customized Commercial Software (COTS)

Below are the minimum requirements that must be considered in the acquisition of COTS:

- **Total lifecycle cost.** This cost includes initial costs such as purchase, installation and training, plus the on-going cost of maintenance and support.

- **Maintainability.** This criterion addresses the ability to administer and perform corrective, adaptive or perfective maintenance on the COTS product within defined tolerance for cost and service, using vendor and/or internal support. This criterion includes minimal operational disruptions and downtime, the ability to tune the software to improve efficiency and effectiveness and the cost and effort to upgrade to improved versions of the software product.

- **Interoperability.** This criterion seeks to minimize the additional support required to integrate the COTS product as a functioning component in the County IT portfolio. As an example, the exchange of information between potentially heterogeneous systems can be facilitated through open standards or non-proprietary protocols (e.g.,
TCP/IP). Interoperability should include flexibility in supporting changes over time and among multiple state agencies and systems. Interoperability standards affecting more than one Agency shall be mutually determined and consistent with all higher-level (e.g., Statewide) standards.

- **Portability.** This criterion addresses the ability of an existing software component to move from one physical or logical position in the IT infrastructure with minimum impact on cost and service.

- **Scalability.** This criterion ensures that acceptable COTS software products enhance the ability of the system to support future growth and increased throughput necessary to meet e-Government goals. This objective is achieved through excess capacity or the flexibility to easily modify and/or enhance the system as needed (e.g., application performance or transaction process speed, forward and backward compatibility, modularity, etc.).

- **Availability/Accessibility.** This criterion seeks to maintain a system's operational readiness and required level of service without disruption from software failure. This is achieved through robust and/or redundant (e.g., fault tolerant) software. Operational readiness will include the ability of users and operators to access the system, in a timely fashion, to perform its intended functions.

- **Reusability.** This criterion addresses the ability to make repeated use of the COTS software product for additional requirements with minimum additional cost.

- **Functionality/performance.** This criterion seeks to guarantee that the County Operational requirements, especially its mission critical requirements, intended to be performed by IT systems, can be achieved effectively and efficiently with the specified COTS software. It includes the properties of efficient software/hardware integration that affects the ability of the overall system to perform adequately to meet operational requirements.

- **Security.** This criterion addresses the need to protect system data and the operational environment from loss or compromise. It includes the ability of the COTS software to prevent and contain malicious as well as non-malicious security breaches.
• **Other Specific Criteria.** Other criteria are explicitly used for specifying the acceptable set of COTS software products. For example, vendor viability, licensing restrictions, potential product market share, customer recommendations, and product volatility (e.g., frequency of upgrades and potential obsolescence) may be important.

  b. Open Source Software

Open software enables access to the source code written in the programming language in which the special-purpose software is written, which allows the expert users to read, modify and adapt the open source software to current purposes. Open software is at the same time computer software whose source code may be freely redistributed and modified.

In acquiring Open Source Software the ICT Directorate shall:

1. Develop a detailed technical OSS specification that meet the client needs

2. Identify the Open Source Software that could provide solution for the target information system

3. Solicit and evaluate various OSS offers in the market.

4. Consider licensing that come with OSS

c. Application software

Application software is computer software designed to help the user to perform singular or multiple related specific tasks. Examples include enterprise software, accounting software, graphics software, office productivity software, utility software, security software, web development and management software, database software, communication software, network management software and media players.

ICT Directorate shall ensure that:

• The latest stable versions of application software are installed in user computers and that security and software updates are made as soon as they are released. Where a previous version is to be used adequate justifications are to be provided.

• Users are adequately trained on the use of any application software purchased.
- All application software acquired are adequately supported and maintained by the vendor.

### 8.4. SOFTWARE DEVELOPMENT

County shall encourage the development of custom software applications where necessary. Custom software or bespoke software is software that is specially developed for the client. It contrasts with the use of software packages developed for the mass market, commonly referred to as commercial off-the-shelf (COTS) software, or free software. Custom software can be developed by County in-house software development group, or be commissioned from a software house or independent software developer.

Custom software can accommodate the County’s particular preferences and expectations. They may also be designed stage by stage to take into account all issues including those not mentioned in the specifications.

It is recommended that an optimal system development methodology such as software development lifecycle be adopted in order to obtain a useful system. In addition, a software development process must adhere to project management principles as they may be defined in the Project Management Guidelines.

#### a. System Development Process

The System Development process encompasses all activities involved in the development of application systems. Such activities include requirements gathering, analysis, design, construction, testing, implementation, and maintenance.

The County shall use SDLC in developing applications in a well-defined, disciplined, and standard approach. It provides a methodological approach and a platform for managing, directing, monitoring and controlling the process of application or software building, including description of the process and deliverables.

To obtain good results from the SDLC methodology, its stages must be strictly followed:

- Requirements gathering and system analysis
- System Design
- Development and Implementation
• System Testing

• Operations and maintenance

• Post implementation monitoring and evaluation

County shall adopt the following methodology which is derived from SDLC and outlines the specific activities in each phase as well as the outputs and deliverables of the stage.

b. Software Development Lifecycle

It is imperative that all software development projects have a comprehensive Project Charter precedent to project initiation. In addition, the processes must adopt a documentation standard including: Context Diagram (CD), Entity Relationships Diagrams (ERD), Data Flow Diagrams (DFD) and Process Maps as appropriate at every stage.

c. Procurement

Procurement of software shall be done with consultation and coordination of the ICT Directorate which shall be responsible for the preparation and issuance of all technical specifications for the software, as well as ensuring that the guidelines stipulated herein are adhered to. County shall use requisition and acceptance forms to ensure that requests for procurement of software are validated by the respective Heads of Department. County shall also ensure that requirements are clearly defined and documented when procuring enterprise software. Where possible, County shall endeavor to use enterprise version of software, depending on the requirements of the user.

County shall make sure that there is no already existing software application within County that provides equivalent functions and that can be replicated in the organization before procuring any software to avoid duplication.

All ICT software procured or donated to County shall be received by the ICT Directorate which shall ensure proper custody and issuance. All donations shall be required to meet the minimum specifications. Furthermore, all software assets (new, transferred and/or written off) shall be recorded by the ICT Directorate for audit and other managerial purposes.

County shall endeavour to procure and use the latest version of software. Where a previous version of software is to be used, the user shall be required to give justifications.
Technical evaluation shall be undertaken to ensure that the software is fit for the purpose it is being acquired for and that it meets the provided specifications. Upon delivery of the software, ICT Directorate shall inspect and ascertain that they meet the laid down specifications. The ICT Directorate shall ensure that technical evaluation and inspection reports are prepared respectively.

The ICT Directorate shall ensure that an agreement is in place to warrant software support and replacement when required, and that such agreements acquired are enforced. When the software is procured, related licenses should be adhered to, and that the vendor should guarantee subsequent licensing arrangements.

The procurement procedures as stipulated in the public procurement and disposal act 2005 shall be followed.

d. Maintenance

ICT Directorates shall keep an inventory of all software in the County, and give quarterly reports on status of utilization, support, adaptability and licensing status.

ICT Directorate shall also determine which software have expired licenses for the purposes of renewal, upgrade or disposal. Where such systems have proprietary data, that data shall be extracted using suitable mechanisms.

Software media and administration documentation, whether hardcopy or electronic, shall be securely stored in a central repository and copies may be created for backup and disaster recovery purposes as permitted by the license terms and conditions. Software media shall be tagged with the standard government labeling conventions and appropriately physically secured.

Software maintenance shall be done in-house by ICT Directorates who shall develop a maintenance schedule on upgrading and debugging. Sub-contracting for software maintenance shall be through appropriate justification and approval by the ICT governance committee. Due diligence shall be undertaken in retaining such contractors. The ICT Directorate shall prepare an annual maintenance report and forward it to the ICT governance committee.
e. Disposal

The ICT Directorate may justifiably replace software with newer versions or replace no longer required software for various reasons:

- Replacement by a newer version
- No longer used in the department
- Obsolescence
- All retired software may be destroyed in accordance with manufacturer end-user license agreements and copyright laws or donated to innovation centers for further research on software re-use. Generally, if the software is to be discarded, media should be damaged to prevent subsequent unauthorized use.
- Upon retirement of computer equipment, all software and data must be removed from computer hard drives to ensure software license compliance, user privacy, and the security of institutional data.
- The ICT Directorate on assessment of the software may advice on transfer of software ownership, retirement or redistribution to another location within County.

8.5. Prohibited Software

Prohibited software are software that can cause malicious damages to County systems, networks and data, those that violate other organization’s licensing requirements or that which interfere with County network throughput.

It is expressly forbidden to possess, distribute, reproduce or use computer programs for reasons such as scanning networks, intercepting information or password capture unless specific authority is obtained or held.
8.6. Software copyright compliance
1. The County will only use a genuine copy of legally acquired software that is configured and used in accordance with the license terms and conditions as set out by the copyright holder.

2. The making or use of unauthorized or illegal software copies is prohibited in the County. Where possible, controls will be in place within the County to prevent the making or use of unauthorized or illegal software copies. These controls shall include effective measures to verify compliance with acquired software licenses.

8.7. Software Audits
County shall periodically conduct audit of software in County, to ensure that they comply with all software licenses and the software developed meet the required guidelines.

8.8. Training and Knowledge Transfer
County shall ensure that ICT officers mandated to maintain or support software acquired are adequately trained. Where a maintenance contract is in place, County shall ensure that measures are put in place to enforce knowledge transfer to ICT officers by contractors and vendors for continuous support and maintenance of the system once the contract expires.

8.9. Software Custody
1. ICT Directorate shall have custody of all software under a documentation library.

2. ICT Directorate shall facilitate training on the acquired software.

3. The County staff shall not borrow or lend any software.

4. All software developed in house by the County staff shall become property of the County.

8.10. Licenses
1. The County shall comply with all laws regarding intellectual property. This applies to all software licensed or developed by ICT staff at/and for the County.

2. The County shall negotiate for corporate licenses for use by all departments.

3. All purchased/customized software must be accompanied by the required licenses as per specifications.
4. All licenses must be in the name of Department/County.
5. All purchased/customized software shall be delivered with documentation.
6. All software revision shall be accompanied by documentation.