MURANG'A COUNTY GOVERNMENT

INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

DRAFT

NOVEMBER 2024.

FOREWORD

Information and Communication Technology (ICT) is an important enabler for County to achieve its strategic, tactical and operational goals. The need to automate business processes and emerging sophistication of cyber security breaches in the world have shifted the emphasis of focus by organizations from acquisition, deployment, use of software and decommissioning of ICT resources.

The current ICT policy was approved in June 2013 and reviewed in June 2017. Since then there have been a myriad of changes to the operational, regulatory and legal environment. During implementation of the policy, it was also noted that there were gaps in compliance to some of the ICT thematic areas such as ICT governance, System and Applications, Information security and IT infrastructure.

The Government of Kenya (GoK) through the Information Communication Technology (ICT) Authority has issued several ICT Standards that public entities are required to adopt and operationalize. Besides, several laws and regulations have been enacted to regulate the ICT industry. Further, there is need to align ICT policy to the requirements of ISO/IEC ISMS standard which has been adopted by County.

This ICT policy seeks to establish clear guidelines for optimal acquisition, deployment, management and decommissioning and/or disposal of computing resources. The policy has outlined broad guidelines for ICT governance, ICT infrastructure, systems and applications, website management, Internet use, email management, information security, cloud computing, business continuity, ICT human capacity and acceptable use of computing resources.

The policy has provided monitoring and evaluation framework to assess the level of compliance with policy provisions for smooth implementation. The policy will be reviewed every three (3) years or as need arises to take cognizance of changes in the operating environment, technological changes, business requirements and changes in the regulatory and /or legal requirements.

CECM in Charge ICT

PREFACE

In the modern age where technology influences every aspect of our lives, adoption of technology in organizations is paramount and creating institution-wide systems necessitates a solid policy framework. ICT being an enabler in all facets of business operations requires investment in ICT as a critical success factor in implementation of the County's mandate.

The policy is an evolving document which requires revision and updates to align to emerging changes arising from new laws, regulations, standards, circulars and policies from The Government and relevant bodies.

The ICT Policy establishes guidelines and protocols for the effective and secure use of technology resources within the County. It also seeks to promote efficiency, security, and compliance with the following GOK regulations:

The policy has incorporated guidelines that are required to enhance controls, operational efficiency and effectiveness.

The policy will serve as a central guide employee including those on contract, casuals, interns, trainee employees and related parties in ICT operations and decision making.

This Policy shall be effective from 1 January 2025 and will be amended periodically on need basis.

Irungu Kang'ata

Governor Murang'a County

Table of Contents

ABBREVIATIONS AND ACRONYMS

BCP	Business Continuity plan
E-waste	Electronic waste
GoK	Government of Kenya
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IP	Internet Protocol
IP PBX	Internet Protocol Private Branch Exchange
ISMS	ISO/IEC 27001 Information Security Management Systems Requirements
LAN	Local Area Network
MCA	Marketing Communication and Advertising
M&E	Monitoring and Evaluation
MIS	Management Information System
SLA	Service Level Agreements
UAT	User Acceptance Test
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network

GLOSSARY OF TERMS

Encryption	Is conversion of data into a format that is not easily understood by unauthorized people.
Extranet	A private network such as the intranet that has been extended to users outside the organization. The users outside the organization are usually the partners.
Malware	Malicious software that have been designed to spy on which sites you are visiting without you knowing in order to target adverts towards you.
Software patch	A piece of software designed to update a computer program or its supporting data, to fix or improve it.
Server	A networked computer that is providing a specific service to other computers on the network.
Spam	Sending massive amounts of electronic junk mail that people haven't asked for.
System administration	Is a role that deals with the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers.
Web content approver	A person charged with the responsibility of reviewing content from writers to ensure that it conforms to the corporate communication policy before upload by the web master.
Virus	A computer virus is a piece of program code that, like a biological virus, makes copies of itself by attaching itself to another program. Usually dangerous to computers and network systems.
Emerging Technologies	Emerging technologies are technologies whose development, practical applications, or both are still largely unrealized, such that they are figuratively emerging into prominence from a background of non-existence.

CHAPTER ONE

INTRODUCTION

1.1. Background

1.1.1 Establishment of COUNTY

1.1.2 Mandate

The mandate of County is

1.2. ICT Function

ICT is a key driver of the County's business processes. The ICT Function is charged with responsibility of promoting the use of ICT in delivery of services towards realization of County's mandate. The key functions are to:

i. Formulate, review and implement ICT policy and strategy.
ii. Deploy suitable systems anchored on the business needs for efficient service delivery.
iii. Provide appropriate, effective and efficient ICT services to COUNTY and manage information systems and services accordingly.
iv. Maintain and update the Management Information System (MIS) for the collection, analysis and dissemination of data within COUNTY.
v. Oversee the management of ICT infrastructure and promote effective business systems that are cost-effective.
vi. Ensure continuous upgrade of software and setup of supporting network infrastructure.
vii. Design and update an interactive web database from information gathered from other functional areas and implement E-commerce solutions.
viii. Ensure secure, continuous uninterrupted availability and functionality of computer systems.
ix. Ensure enhancement of new technology as per the trends which are cost effective and value adding to COUNTY.
x. Provide user support and maintenance;
xi. Ensure ICT security and risk management

1.3. Rationale

The global technological advancements demand the use of ICT to support organizations operate efficiently and effectively. ICT plays a vital role in supporting organizations towards realization of their mandates. This role has been buttressed by Sustainable Development

Goals, Africa Agenda 2063, the Kenya Vision 2030, and the Bottom-Up Economic Transformation Agenda (BETA). The rationale of this ICT policy is to promote provision of accessible and reliable ICT resources, to comply with the legal and regulatory frameworks and to ensure staff are provided with adequate ICT equipment, systems and skills.

1.4. Scope of the policy

This policy covers ICT governance, ICT infrastructure, systems and applications, website management, Internet use, email management, information security, computing, business continuity, ICT human capacity and acceptable use of computing resources. The Policy applies to the County Members, members of staff, interns, and other County stakeholders.

1.5. Legal, Policy, and Administrative Framework and Standards

This policy shall comply with the Constitution of Kenya 2010, Executive orders issued from time to time by His Excellency the President and other applicable legislations, regulations, standards, policies and procedures. This include but not limited to:

(a) Constitution of Kenya 2010.
(b) Kenya Information and Communication Act (2018).
(c) Access to Information Act, No 31 of 2016.
(d) Data protection Act No. 24 of 2019.
(e) Computer misuse and Cybercrime Act, 2018.
(f) Public Finance Management Act, 2012.
(g) Public Procurement and Asset Disposal Act (2015).
(h) Public Archives and Documentation Service Act, 2012.
(i) Occupational Safety and Health Act (2007).
(j) Government ICT Standards ICTA-2023.
(k) ISO 9001:2015 International Standard.
(l) ISO 27001:2022 Information Security Management System Standard.
(m) Information Technology Infrastructure Library (ITIL).
(n) Control Objectives for information and Related Technology (COBIT) which defines the IT Governance framework and standards.
(o) National ICT Policy (2019).
(p) National E-waste Policy (2018).
(q) National Information Communication and Technology (ICT) Policy Guidelines, 2020.
(r) Any other relevant, laws, regulations and policies.

1.6. Roles and Responsibilities

For the purpose of approval and implementation of this policy, the roles and responsibilities be as follows:

1.6.1. The County

The County shall approve the ICT policy and provide oversight in its implementation.

1.6.2. Senior Management Team

The senior management team shall provide overall coordination of the ICT Policy implementation, monitoring, evaluation and review.

1.6.3. The ICT Function

The Function shall provide technical support and advisory services on ICT matters as stipulated in this Policy.

1.6.4. Staff and stakeholders

The staff and stakeholders shall familiarize with this policy and abide by the respective policy provisions.

1.7. Application

This policy applies to the County, members of staff, interns and other stakeholders.

CHAPTER TWO

ICT GOVERNANCE

2.1. Introduction

ICT governance is an element of corporate governance aimed at improving overall management of ICT within the county to ensure improved value from investment in ICT. The ICT governance will ensure Return on Investment in ICT projects. This will enable the County to give strategic direction, monitor services, mitigate internal and external risks and ensure set objectives are achieved. ICT Governance encompass corporate culture, structures and policy frameworks that influence transparency and accountability in the use of ICT.

2.2. Purpose

The main purpose of this policy area is to define ICT function, the governance structures and frameworks for efficient and effective use of ICT investments.

2.3. Scope

This policy area focuses on alignment of ICT processes with corporate strategic plan, ICT governance, resource management and risk management.

2.4. Policy statement

The ICT governance policy area shall provide strategic leadership, establish County ICT priorities and policies by ensuring an acceptable level of accountability and transparency in ICT operations and investments in accordance with GoK ICT Governance Standard and other industry best practices.

2.5. Policy guidelines

2.5.1 ICT matters shall be handled by a committee at the Board level.
2.5.2 The structure of the ICT function shall be aligned to the GoK ICT governance standard.
2.5.3 The County shall set up an ICT steering committee at the management level in line with GoK ICT governance standard to provide oversight to issues related to ICT.
2.5.4 The County shall ensure that there is sufficient and relevant capacity to manage ICT services and projects.
2.5.5 The County shall develop, implement and evaluate service level agreements (SLAs) with all ICT service providers.
2.5.6 The County shall develop and implement maintenance plans for ICT equipment.
2.5.7 The County shall ensure that ICT projects are implemented as per the GoK ICT project management standards.
2.5.8 The County shall establish an ICT service desk management system.
2.5.9 The County shall develop and implement an ICT strategy that is aligned to the Corporate Strategic plan.

2.5.10 The County shall implement ICT related provisions in the enterprise risk management framework.

2.5.11 ICT Function shall develop, disseminate and monitor a service charter for ICT enabled services.

2.6. Enforcement

The Board of the County shall be responsible for implementation and compliance of this policy area.

CHAPTER THREE
ACCEPTABLE USE OF ICT

3.1. Introduction

The County utilizes ICT infrastructure to deliver products and services to its customers. The County shall promote a culture of professionalism, integrity and ethical use of ICT resources.

3.2. Purpose

The main purpose of this policy area is to outline desirable and undesirable practices in use of ICT resources.

3.3. Scope

The policy area covers the use of the County's information, electronic, computing devices and network resources.

3.4. Policy statement

COUNTY shall ensure acceptable use of its information resources, computing systems, and networks in compliance with the set policies and guidelines.

3.5. Policy Guidelines

3.5.1 Electronic resources shall be used for the purpose for which they are intended.

3.5.2 Users shall respect the rights and privacy of other users.

3.5.3 Users shall adhere to the confidentiality rules governing the use of password and accounts, details of which shall not be shared.

3.5.4 Users shall be prohibited from unauthorized connection of monitoring devices/equipment to the County ICT infrastructure.

3.5.5 Misusing, disclosing without proper authorization or altering information shall be prohibited.

3.5.6 The County's email account shall be used primarily for official business-related purposes.

3.5.7 Copyrighted material shall not be distributed, copied or published in any form without consent of the originator.

3.5.8 The data and information created by users using the County's ICT resources shall remain the property of the County.

3.5.9 Members of staff shall exercise good judgment regarding the reasonableness of personal use of ICT resources.

3.5.10 The County reserves the right to check compliance on software installed in users' devices in accordance with software policy.

3.5.11 Emails from the County domain shall contain a disclaimer stating that the opinions expressed are strictly the originators and not necessarily those of the County.

3.5.12 Users shall exercise caution when opening e-mail attachments received from unknown senders, which may contain viruses.

3.5.13 The County's network shall not be used for the following purposes;

3.5.13.1 The creation, dissemination, storage and display of obscene or pornographic material, hate literature, materials that promote criminal activities, defamatory materials or materials likely to cause offence to others.

3.5.13.2 The creation, dissemination, storage and display of any data that is illegal including, but not limited to, national laws and regulations.

3.5.13.3 Deliberate interference with or gaining illegal access to user accounts and data including viewing, modifying, destroying or corrupting the data belonging to other users.

3.5.13.4 The users of the County ICT resources are prohibited from engaging in the following:

3.5.13.4.1 Illegal activities

3.5.13.4.2 Commercial activities.

3.5.13.4.3 Breach or disruption of network communication.

3.5.13.4.4 Unauthorized use, or forging, of email header information.

CHAPTER FOUR

ICT INFRASTRUCTURE

4.1 Introduction

ICT infrastructure is an essential component in improving productivity, efficiency and the delivery of ICT services. It provides a platform for accessing and interacting with systems and applications. ICT Infrastructure includes end-user devices, networks, telephony and data centers acquired and maintained by the County. The end user devices include desktops, laptops, printers, projectors and tablets. ICT networks include LANs, WLANs, WANs and internet access. Telephony includes IP-PBX, mobile and landline telephone systems that are in use throughout the County. The data center components include servers, storage systems, power backup, cooling and fire suppression equipment.

4.2 Purpose

This policy area provides a framework through which the County shall acquire, deploy, maintain and dispose ICT infrastructure.

4.3 Scope

This policy area covers end-user devices, networks, telephony and data centers acquired and maintained by the County.

4.4 Policy statement

All ICT infrastructure for the County will be acquired, managed and controlled by the ICT department.

4.5 Policy guidelines

4.5.1 ICT Networks and telephony

ICT networks are defined as the medium used to transport data and encompass the aspects of communications protocol used, scale, topology and the devices used to ensure efficient transfer of data from one point to another in the network.

ICT function Shall:

4.5.1.1 Deploy and maintain a high-performance LAN and WAN interlinking the various offices of the institution.
4.5.1.2 Deploy and maintain a suitable voice over internet protocol (VoIP) infrastructure.
4.5.1.3 Maintain up to date documentation of network designs and configurations.
4.5.1.4 Segment Network into sub-networks to isolate various functional areas.
4.5.1.5 Review adequacy of ICT networks every three years or when need arises.
4.5.1.6 Deploy a Virtual Local Area Network (VLAN) for guests.
4.5.1.7 Ensure that network cabling is protected from unauthorized interception or damage by ducting.
4.5.1.8 Ensure use of at least cat 6A Ethernet cables.
4.5.1.9 Configured firewalls, network separation and network monitoring tools.
4.5.1.10 Ensure proper labeling and cable management in the network's cabinet.

4.5.1.11 Regularly monitor network performance to detect bottlenecks, latency issues, or downtime

4.5.2 Data center(s)

The following guidelines shall be applied for the acquisition, use, management and disposal of data center infrastructure.

4.5.2.1 Acquire, deploy and maintain adequate data center infrastructure in accordance with the GoK Data Center Standard.
4.5.2.2 Ensure suitable location to minimize environmental hazards.
4.5.2.3 Secure with robust physical security including but not limited to access controls, surveillance control and burglar proof.
4.5.2.4 Maintain a log of all personnel accessing data center.
4.5.2.5 Redundant power distribution unit and cooling shall be used to prevent single point of failure.
4.5.2.6 Data center shall be restricted to authorized access.
4.5.2.7 Maintain temperature and humidity levels recommended by equipment manufactures to prevent equipment damage.
4.5.2.8 Install fire suppression systems.

4.5.3 End user Computing devices

End user devices such as personal computers, printers and mobile phones are critical assets to access business information systems. Therefore, their adequacy, and reliability enhances effectiveness of office operations and service delivery

4.5.3.1 The County shall endeavor to acquire and maintain suitable end user computing devices.
4.5.3.2 The County shall properly dispose of end user computing devices at the end of their useful life.
4.5.3.3 The ICT function shall develop and implement end user computing devices matrix for all cadres in liaison with departmental needs.
4.5.3.4 The ICT function shall consolidate, compile and prepare technical specifications.
4.5.3.5 The ICT function shall verify and accept end user computing devices.
4.5.3.6 The ICT function shall schedule and carry out quarterly preventive maintenance.
4.5.3.7 End users shall report faulty, damaged or lost ICT equipment to the Head ICT department.
4.5.3.8 The ICT function shall recommend end user equipment due for disposal in accordance with Public Procurement and Asset Disposal Act (PPAD), 2020.
4.5.3.9 The ICT function shall ensure that requests for procurement and acceptance of ICT equipment are validated by Heads of Department (user department).
4.5.3.10 The ICT function shall maintain an up to date inventory of ICT assets.
4.5.3.11 The ICT function shall authorize use of end user devices outside COUNTY offices for employees and any other applicable stakeholder.
4.5.3.12 End user devices taken outside the office shall not be left unattended in public places.

4.5.3.13 There shall be a maintenance contract for End user devices. Manufacturer's instructions and recommendations for maintenance and use of equipment shall be observed at all times.

4.5.3.14 Employees shall handover all the end user device(s) allocated to ICT Unit on separation or redeployment.

4.5.3.15 The ICT function shall ensure Active end user devices are insured.

4.5.3.16 Maintenance of end user devices in accordance with preventive and corrective maintenance procedures.

4.5.3.17 When End user devices are being disposed of, the data shall be totally erased to an unrecoverable state.

4.5.3.18 Ensure depreciation of End user devices is as per the finance policy and procedure manual and asset management policy.

4.5.4 Enforcement

The Head of the ICT function shall be responsible for implementation and compliance of this policy guidelines.

CHAPTER FIVE
SOFTWARE ACQUISITION, MAINTENANCE AND DECOMMISSIONING

5.1 Introduction

Software comprises the entire set of programmes and routines associated with operations of computing devices. The software includes but not limited to operating systems, office applications, Enterprise Resource Planning, collaboration applications

Systems and applications act as enablers to improve productivity of the County's core services. The County is committed to ensuring that the right systems and applications software are in place and maintained. It is important to identify the right systems and applications before undertaking installation, customization, testing, training, commissioning and utilization.

The County has over the years invested substantial resources towards the realization of automation of its operations. The County is committed to continually deploy and maintain systems and applications seamlessly integrated towards realization of maximum return on investment. Software comprises the entire set of programmes and routines associated with operations of computing devices. The software includes but not limited to operating systems, office applications, Enterprise Resource Planning, collaboration applications

5.2 Purpose

The purpose of this policy area is to provide guidance on planning, acquisition, deployment, use and decommissioning of systems and applications.

5.3 Scope

This policy area covers all systems and applications owned or leased by the County.

5.4 Policy statement

This policy area seeks to ensure that systems and applications are planned, deployed, managed and decommissioned in accordance to GOK systems and applications standard

5.5 Policy guidelines

The ICT function shall;

5.5.1 Undertake system analysis and develop technical specifications.
5.5.2 Determine the means of acquisition; commercial off-the-shelf, in-house developed, out-sourcing or open source.
5.5.3 Ensure all software have valid license for proper installation and upgrades.
5.5.4 Ensure software/patches/upgrades is tested before deployment.
5.5.5 Ensure that software is tested to meet the technical specifications and requirements.
5.5.6 Test data shall be selected carefully, protected and controlled.

5.5.7 Ensure that both technical and end-user training is conducted pre and during implementation and on need basis.
5.5.8 Ensure that user acceptance test is carried by process owners and system users.
5.5.9 All suppliers of systems and applications shall sign a non-disclosure agreement with the County.
5.5.10 Installation of any software in the County devices shall be undertaken by ICT staff.
5.5.11 Ensure patches are deployed in a manner that minimizes service disruption.
5.5.12 Ensure that software integration is done in line GoK ICT systems and application standard.
5.5.13 The Head of the user functional area shall signoff after successful deployment of a system.
5.5.14 De-commission obsolete software or no longer supported by developers and vendors.
5.5.15 Ensure that system documentations and source codes are surrendered to the County as per the contractual agreement.
5.5.16 Continuously identify, assess and evaluate adoptability of emerging technologies through participation in events and conferences that showcase emerging technologies.
5.5.17 Benchmark with similar organizations that have adopted emerging technologies.
5.5.18 Evaluate compatibility of emerging technologies with the technology already in use.
5.5.19 Assess availability and sustainability of the emerging technologies in terms of cost and technical capacity.
5.5.20 Acquire new technologies in line with the County's ICT hardware and software policy.
5.5.21 The deployment & integration of the new technologies shall be done by the ICT function.
5.5.22 Training of staff on new technologies shall be done in line with the County's ICT training and capacity building policy.
5.5.23 Sensitize staff to understand, commit to and accept the new technology.
5.5.24 Maintain service level agreements of new technologies in line with County's ICT governance policy.

5.6 **Enforcement**

The Head of the ICT function shall be responsible for implementation and compliance of this policy guidelines.

CHAPTER SIX

WEBSITE MANAGEMENT

6.1 Introduction

Website is a major source of information for both internal and external stakeholders. COUNTY endeavors to develop, maintain and manage its website to meet the needs of its stakeholders. COUNTY shall put in place measures to promote its proper management and acceptable use.

6.2 Purpose

The purpose of this policy area is to guide the design, development, maintenance and management of a user-friendly website.

6.3 Scope

This policy area covers development, hosting, content management and maintenance of the county's websites, web-based applications and documents made available through the domain https://muranga.go.ke/ and its subdomains.

6.4 5.4 Policy statement

The county's website shall provide accurate, useful, timely and up to date information on all aspects of service provision.

6.5 Policy guidelines

COUNTY shall;

6.5.1 Establish a website management committee to coordinate management of the County's website.
6.5.2 Ensure design of all web pages conform to the technical and design requirements.
6.5.3 Ensure that all web pages are viewable in compatible web browsers, operating systems and devices.
6.5.4 Ensure the websites is developed, managed and maintained in accordance with GoK ICT standards.
6.5.5 Ensure website is developed using Content Management Systems (CMS).
6.5.6 The Head of Marketing and Communication shall be responsible for the county's websites content.
6.5.7 Ensure the website is in conformity to the county's Brand Manual.
6.5.8 Ensure the website is hosted securely.
6.5.9 Monitor the county's website's availability to ensure 99.99 uptime.
6.5.10 Ensure the website is user friendly and accessible on all devices.
6.5.11 Ensure that accessibility of web content is adapted to meet the needs and preference of different people.

6.6 Enforcement

The Head of the ICT function and Communication shall be responsible for implementation and compliance of this policy guidelines.

CHAPTER SEVEN

INTERNET USE

7.1 Introduction

Internet connectivity is critical in facilitating the county's business operations. Therefore, the county shall ensure the internet service is available, reliable and secure. The County reserves the right to manage access to Internet content.

7.2 Purpose

The purpose of this policy area is to outline rules and procedures for the proper use of internet services, as well as guidelines for their provision.

7.3 Scope

This policy covers acquisition, provision, usage and management of the internet, extranet and intranet for the county's operations.

7.4 Policy Statement

The County shall at all times ensure availability of quality, reliable, secure and accessible internet, extranet and intranet services for all users.

7.5 Policy guidelines

7.5.1 The ICT Function shall maintain quality and reliable internet services from credible and competent Internet service providers.

7.5.2 The ICT Function regularly and randomly monitor the bandwidth capacity to determine adequacy and value for money.

7.5.3 Members of the County, employees and other stakeholders engaged by the county shall use the internet responsibly in accordance with the acceptable use policy.

7.5.4 The ICT Function shall provide extranet and intranet to facilitate ease in service delivery.

7.5.5 The ICT Function shall ensure all Internet connection shall be implemented through a firewall.

7.5.6 Users shall bear personal liability for any copyright violation or infringement while using the county's internet.

7.6 Enforcement

The Head of ICT shall be responsible for implementation and compliance of this policy guidelines.

CHAPTER EIGHT

EMAIL MANAGEMENT

8.1. Introduction

An electronic mail (E-mail) management system is a platform that allows users to send, receive, and manage electronic communications. This policy aims to enhance internal and external communication.

8.2. Purpose

The purpose of this policy is to guide on provision of official email accounts and appropriate use of the email service within and without County facilities.

8.3. Scope

This policy covers acquisition, creation, usage and termination of official email accounts.

8.4. Policy statement

8.4.1 The county shall provide a secure email platform for official communication.
8.4.2 Use of email services shall adhere to legislation, policies and procedures on ethical and professional conduct.

8.5. Policy guidelines

8.5.1 All County of directors and employees and other authorized persons shall be facilitated with a the county's email account in the standardized format of firstname.lastname@muranga.go.ke.
8.5.2 All electronic mail shall be centrally available from a mail server.
8.5.3 Users shall be granted e-mail accounts once an official request has been made to the Head of ICT.
8.5.4 All use of email shall be consistent with the acceptable use policy.
8.5.5 Employees and other authorized persons shall seek approval before sending an email broadcast.
8.5.6 All correspondences and circulars sent, received, forwarded or other shared on the county's individual staff or group emails shall be taken as duly and officially communicated.
8.5.7 Email accounts for users on transfer/exiting service will be deactivated within 24 hours upon confirmation by the Head of Human Capital.
8.5.8 Information contained in the deactivated account will be archived for future reference.
8.5.9 Users shall observe email etiquette.

8.6. Enforcement

The Head of ICT shall be responsible for implementation and compliance of this policy guidelines.

CHAPTER NINE

INFORMATION SECURITY

9.1 Introduction

Information security is critical in ensuring integrity, confidentiality and availability of information and information assets. The county shall ensure that adequate information security is in place for its ICT infrastructure, systems and applications, and personnel interacting with the ICT resources.

9.2 Purpose

This policy provides a mechanism to secure ICT infrastructure, systems and applications in order to manage and safeguard confidentiality, integrity and availability of the information assets.

9.3 Scope

This policy area covers all network systems and devices that form the ICT network infrastructure; access control, password management, physical and environmental, human resource, incident management, acceptable use, BYOD, mobile devices, teleworking, applications securities and ICT asset management, backup, cryptographic control, network securities, anti-malware.

9.4 Policy Statement

The county shall establish and continually improve the security measures of its information assets and review effectiveness of security measures in place to ensure conformity to GoK ICT standards on Information security.

9.5 Policy Guidelines

Physical and Environmental Security

9.5.1 The county shall install access control systems and physical locks for the designated areas. Only authorized personnel shall be allowed access to the secured areas.

9.5.2 The county shall ensure data center, networks and cloud computing are set up in accordance with the GoK Information security standard.

9.5.3 The Head of the ICT function shall authorize all requests for access to information processing facilities on a need basis. Such persons shall be escorted by authorized personnel.

9.5.4 The county shall ensure installation of clean power to protect ICT equipment from damage.

9.5.5 All ICT equipment shall be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.

9.5.6 A record of access to Information processing facilities such as log books shall be maintained.

9.5.7 Information processing facilities shall at all times be under surveillance systems.

9.5.8 ICT equipment shall be installed, used, stored and maintained as per manufactures' guidelines.

9.5.9 Installation, disconnection and modification of ICT equipment shall only be performed by authorized ICT personnel.

9.5.10 Smoking, eating and drinking is prohibited in information processing facilities.
9.5.11 Quarterly preventive schedules shall be implemented for information processing facility equipment.

Network Security

9.5.12 Head of the ICT function shall ensure that physical and logical design of the network is documented and all the network changes are updated.
9.5.13 Configuration of network devices shall be documented and aligned with industry best practice. This shall include changing any vendor-supplied defaults (passwords, configurations, etc.) before installing in production.
9.5.14 There shall be effective and properly configured firewalls.
9.5.15 Shared network administration accounts are prohibited.
9.5.16 Carry out periodic network audits in line with GoK ICT audit standards to identify any vulnerabilities such as end of life network equipment.
9.5.17 Network intrusion detection systems (IDS) and prevention systems shall be implemented and monitored.
9.5.18 End-of-life or unsupported network devices shall not be used in the county network system
9.5.19 The county shall ensure logical networks are properly segmented and/or segregated.
9.5.20 The county shall put in place work monitoring tools to ease network management and deter network security breaches.
9.5.21 All ICT devices shall be set up with the principle of least privilege whereby access is provided only to authorized users.
9.5.22 Data in transit within the county systems shall be secured through encryption protocols in compliance with all relevant agreements, legislation and regulations or as defined by industry best practices.
9.5.23 Power cables shall be segregated from communications cables to prevent interference.
9.5.24 Cables and equipment shall be clearly marked to minimize handling errors such as accidental patching of wrong network cables. A documented patch list shall be used to reduce the possibility of errors.
9.5.25 Remote access to the County's' information systems shall only be allowed through an authorized secure connection such Virtual Private Network (VPN).

Logical Security

9.5.26 Access rights and privileges to information systems and applications shall be assigned based on user roles and responsibilities.
9.5.27 The access rights of all staff, third party users to information and information processing facilities shall be revoked within 24hrs upon notice of termination of their employment, contract or agreement, or adjusted upon change.
9.5.28 Computers shall automatically log off after 5 minutes when left unattended or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended.

9.5.29 All users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.
9.5.30 System users working remotely shall be identified, authenticated and authorized to access the county's ICT resources.
9.5.31 The competences of users with privileged access rights shall be reviewed regularly in order to verify if they are in line with their duties
9.5.32 The ICT department shall implement reliable measures to safeguard information.

Malware Security

9.5.33 All the county computers and computing devices shall run on the approved, updated and licensed anti-malware software.
9.5.34 Any device that connects to the county network shall have a current antivirus installed and running at all times.
9.5.35 All the county issued computers shall use the antivirus software installed and configured by the ICT department. Users shall be prohibited from disabling or tampering with the installed antivirus software.
9.5.36 The county shall block and remove from its network any computer system or device that has been deemed to be infected by a virus or malware until the threat is neutralized.
9.5.37 All email inbound to the county shall be scanned for malware and spam.
9.5.38 All users shall exercise appropriate caution when opening external websites, emails or attachments.
9.5.39 The county shall seek technical assistance from relevant government agencies in case of a cyber-attack beyond its capacity.

Password Management

9.5.40 Access to the county's ICT resources shall be restricted by use of multiple factor authentication; passwords, passcodes or passphrases.
9.5.41 Passwords shall not be reused on different systems and/or for different roles and privileges in the same systems.
9.5.42 Passwords shall have a minimum of 8 characters with a mix of alphanumeric, special characters and mixed case character: where a particular system will not support 8-character passwords, then the maximum number of characters allowed by that system shall be used.
9.5.43 All devices shall be password protected.
9.5.44 Passwords shall be kept confidential and shall not consist of well-known or publicly posted identification information. End users shall be responsible for the confidentiality of their passwords.
9.5.45 Systems shall be configured to prohibit users from re-using the last 3 previously used passwords.
9.5.46 Users shall not us the "Remember This Password" feature while logging in to applications.
9.5.47 The county employees shall use their provided credentials when accessing shared workstations.

9.5.48 Users shall change their initial/default passwords at the first log on and thereafter 30 days or based on emerging risks or in the event an account or password is suspected to have been compromised.
9.5.49 Failed password attempts shall be limited to three (3)

Human Resource Security

9.5.50 All users of information assets shall undergo Security Awareness Training on User responsibilities and recommended best practices.
9.5.51 Screening shall be undertaken to all individuals or companies hired or contracted to provide any ICT related services within the county.
9.5.52 ICT function shall ensure segregation of duties and areas of responsibilities to reduce the risk of fraud error and bypassing of information security controls.

ICT Supplier Management

9.5.53 Contractual and service level agreements shall include information security obligations.
9.5.54 All third parties shall sign non-disclosure agreements before their granted access to the County's' confidential information.
9.5.55 The County shall maintain an inventory of ICT suppliers and contractors that can impact on information security.
9.5.56 The County shall define Information assets that suppliers can access, monitor, control and use.
9.5.57 Undertake awareness training for County's' personnel dealing with suppliers.
9.5.58 Access rights shall be revoked upon separation of ICT suppliers.
9.5.59 ICT suppliers shall report information security incidents to the county's Head of ICT.

Incident Management

9.5.60 The ICT department shall monitor the general ICT threat landscape, especially for software used by its users and notify the teams responsible for administering these systems to take the appropriate actions when significant threats have been identified.
9.5.61 The ICT department shall maintain an incident log of ICT infrastructure and software.
9.5.62 The ICT department shall analyze incidents for categorization and prioritization.
9.5.63 For minor and moderate incidents, identify and institute appropriate interventions.
9.5.64 For major incidents escalate to relevant authorities.
9.5.65 The ICT department shall determine, document and implement appropriate corrective measures.

Clear Desk

The following policy guidelines apply:

9.5.66 Hot-desking areas shall be left clean, tidy and neat when unoccupied, and at the end of each working day.

9.5.67 All confidential documents shall be removed from desks, stored and locked in lockable furniture when not in use.
9.5.68 In a remote working setting, practical steps shall be taken to ensure documents remain ‘out of reach’ and ‘out of sight’.
9.5.69 Unattended computing devices shall be left in a secure state when working in a shared or public space, this means manually applying the screen lock.
9.5.70 Members of staff shall manually log out of shared computing devices when no longer in use.
9.5.71 Removable media devices shall not be left unattended.

Bring Your Own Device (BYOD) Policy

The following policy guidelines apply:

9.5.72 Any personal devices that cause security vulnerabilities shall be denied access to the County’s ICT resources and services.
9.5.73 The county ICT function shall support the setting up and connection to systems and accounts only where possible.
9.5.74 Staff shall be personally liable for security vulnerability caused by use of personal devices.
9.5.75 The county reserves the right to carry out vulnerability assessment on personal devices accessing its information systems and resources on a need basis.
9.5.76 Users shall take reasonable measures to protect personal devices, used for work related purposes from cyber threats.
9.5.77 In an event a personal device used to access the county’s network infrastructure and information systems is lost, faulty or damaged the user shall notify the ICT Department to take necessary action.

9.6 Enforcement

The Head of ICT shall be responsible for implementation and compliance of this policy guidelines. A breach of security shall be handled in accordance with the county disciplinary procedures and/or the laws where necessary.

CHAPTER TEN
DATA PROTECTION

10.1 Introduction

Data protection ensures personal information of individuals is protected and information technology does not violate human identity, human rights, privacy, or individual or public liberties.

10.2 Purpose

10.2.1 The main purpose of this policy area is to protect and secure all data consumed, managed, and stored in the county.

10.2.2 The policy area provides guidance on how the county will handle the data it collects. It helps in complying with the data protection law, protect the rights of the data subjects and protects the county from risks related to breaches of data protection.

10.3 Scope

This policy area applies to members of the County, employees, stakeholders and any other third party who handle and use the county information. This policy area also applies to all formats of data whether manual or digital.

10.4 Policy Statement

COUNTY shall comply with all relevant Kenyan legislation and in particular Data Protection Act 2019. COUNTY recognizes that the protection of individuals through lawful, legitimate, and responsible processing and use of their personal data is a fundamental human right.

10.5 Principles of Personal Data Protection

10.5.1 Personal data shall be processed lawfully, fairly and in a transparent manner and in line with the right to privacy.

10.5.2 Personal data shall be processed in accordance with the right to privacy

10.5.3 Data shall be collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with that purpose.

10.5.4 Processed data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.

10.5.5 COUNTY shall ensure data is accurate and up to date.

10.5.6 Data shall be processed in a manner that ensures its security using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and accidental loss, destruction, or damage.

10.5.7 Data shall not be transferred out of Kenya unless there is proof of adequate data safeguards/ measures or consent from the data subject.

10.6 **Enforcement**

The Head of the ICT function shall be responsible for implementation and compliance of this policy guidelines. A breach of security shall be handled in accordance with the the county disciplinary procedures and/or the laws where necessary.

CHAPTER ELEVEN

CLOUD COMPUTING

11.1Introduction

Cloud computing has evolved significantly over time to offer business solutions in a flexible ICT environment to suit the changing needs and requirements. Cloud computing is a method of delivering Information and Communication Technology (ICT) services where the customer pays to use, rather than necessarily own, the resources. These services are typically provided by third parties using internet technologies. Cloud services can provide a significant range of benefits to individuals and organizations including increased solution choice and flexibility, faster time to solution, and reduced total cost of ownership. Cloud services are provided via four deployment models: Private cloud, public cloud, Community cloud and Hybrid cloud

11.2 Purpose

This Policy area outlines the principles and guidelines for the use of cloud computing services within the Agency.

11.3 Scope

This Policy area covers the acquisition and deployment of cloud-based products and services whether owned or leased by the County for official use.

11.4 Policy Statement

11.4.1 The County shall ensure cloud-based services comply with Data Protection Act, 2019 and GOK ICT standards on cloud computing.

11.4.2 The County shall leverage on cloud-computing for scalability, mobility and reliability of its services.

11.5Policy Guidelines

11.5.1 The county shall establish the need for cloud-based service.

11.5.2 The county shall define minimum specification requirements for a cloud-based service.

11.5.3 The county shall ensure the cloud-based service provider complies with best industry standards.

11.5.4 The county shall acquire cloud solutions from a list of accredited cloud providers.

11.5.5 A formal non-disclosure clause shall be documented and signed between the county and cloud-service provider.

11.5.6 The county shall reserve the right to audit cloud computing services from the service provider.

11.5.7 Personal cloud service accounts shall not be used for storage, manipulation or exchange of organization related communication of the county's owned data.

11.5.8 Use of cloud computing services shall comply with the internet policy and acceptable use policy.

11.5.9 The county shall ensure there is monitoring of the service level agreement for cloud services.

11.5.10 Cloud-based solutions shall deliver the same or better levels of service as an in-house solution to ensure business continuity, in line with the requirements of the business service being delivered.

11.5.11 Cloud based solutions shall safeguard the security and privacy of the county data and comply with all appropriate security and privacy requirements.

11.5.12 Cloud based solutions will be delivered using the same processes and controls as any other technology solution at the county.

11.5.13 Where there is use of cloud services, private clouds are highly discouraged.

11.6 Enforcement

The Head of ICT shall be responsible for implementation and compliance of this policy guidelines

CHAPTER TWELVE
BUSINESS CONTINUITY

12.1 Introduction
Business continuity is essential in managing potential loss of information or inability to access information in the event of a disaster and internet failure.

12.2 Purpose
The purpose of this policy area is to ensure availability of ICT services in the event of failure of ICT systems or infrastructure.

12.3 Scope
This policy area covers back-up, testing and recovery of systems and Information in line with the Business Continuity and Disaster Recovery Plan.

12.4 Policy Statement
COUNTY shall put in place relevant measures for business continuity to ensure adequate back up facilities are provided for the recovery of data and systems in the event of failure.

12.5 Policy guidelines
The county shall;

12.6.1 Develop, maintain and implement the business continuity and disaster recovery plan.

12.6.2 Ensure that the ICT function develops, maintains, and implements a comprehensive data backup procedure.

12.6.3 Formulate appropriate data backup plans like automation for their information systems.

12.6.4 For safety, backup media shall be stored in a fireproof, waterproof and protected location. In the case of magnetic media, they shall be in a case or vault that is shielded from electro-magnetic radiation.

12.6.5 Establish and maintain an offsite backup location for data and information. The security controls at the offsite backup location shall at the minimum be same as those of the primary site

12.6.6 Establish and maintain a hot site for ICT services.

12.6.7 Testing of backups shall be tested as prescribed in the county procedure on data backups and restoration.

12.6.8 The ICT function shall identify and evaluate ICT risks and provide mitigation measures.

12.6.9 Users shall back up their data on a location identified by the ICT function

12.7 Enforcement

The Head of the ICT function shall be responsible for implementation and compliance of this policy guidelines.

CHAPTER THIRTEEN

ELECTRONIC RECORDS MANAGEMENT

13.1 Introduction

Electronic records are form of records that are machine-readable. They may be any combination of text, data, graphics, images, video or audio information that is created, maintained, modified or transmitted in digital form by a computer or related system.

13.2 Purpose

This policy area will provide guidance for the effective management of electronic records.

13.3 Scope

This policy area covers all processes concerned with management of electronic records at the County.

13.4 Policy statement

13.4.1 The County's' electronic records management shall be in accordance with the Public Archives and Documentation Service Act, 2012.

13.4.2 The County's shall deploy an E-records Management system that adheres to GoK ICT standards on electronic records.

13.5 Policy Guidelines

The following policy guidelines apply;

13.5.1 The County shall establish the E-records management committee.

13.5.2 The ICT function in liaison with records management function shall oversee deployment and management of Electronic Records Management System (ERMS).

13.5.3 ERMS shall be integrated with other Information Systems.

13.5.4 The County shall prepare and implement a digitization plan.

13.5.5 The County in consultation with the Kenya National Archives and Documentation Services (KNADS) shall appraise E-Records for disposition.

13.5.6 E-records and information shall be categorized and classified according to the GoK classification scheme as secret, restricted, confidential, unrestricted or public.

13.6 Enforcement

The Head of the ICT function and the Records Management Committee shall be responsible for implementation and compliance of this policy guidelines.

CHAPTER FOURTEEN

ICT HUMAN CAPACITY DEVELOPMENT

14.1 Introduction

In order to better realize value for its ICT investments, the County shall ensure coherence and relevance of skills is maintained within the organization. A comprehensive ICT human capacity development policy is necessary to facilitate identification of training needs for staff as well as address the ICT literacy needs.

14.2 Purpose

The purpose of this policy area to seek to build requisite ICT capacity for optimal utilization of the ICT resources and services.

14.3 Scope

This policy area addresses basic, intermediate and advanced ICT knowledge, skills and abilities.

14.4 Policy statement

The county shall attract and retain skilled ICT staff, build their capacity through continual training, mentoring, coaching and benchmarking.

14.5Policy Guidelines

The county shall;

14.5.1 Assess the ICT skills gap for ICT staff and end users when need arises and implement the recommendations.

14.5.2 Ensure ICT staff subscribe to ICT professional bodies and actively participate in relevant seminars, workshops and trainings.

14.5.3 ICT projects have a well-defined training plan, capacity building and knowledge transfer.

14.5.4 Ensure adequate ICT staff establishment to support organizational mandate.

14.5.5 Ensure new employees are inducted on appropriate ICT skills.

14.5.6 Ensure User guides and technical manuals are developed for end user and other stakeholders.

14.5.7 Conduct user training when there is a system change that requires skills upgrade.

14.6 Enforcement

The head of the ICT function shall be responsible for implementation and compliance to this policy.

CHAPTER FIFTEEN

IMPLEMENTATION, MONITORING, EVALUATION AND REVIEW

15.1Introduction
An effective implementation, monitoring and evaluation framework will be critical in assessing the level of compliance with policy provisions and smooth implementation of this policy.

15.2 Implementation
The policy implementation plan and ICT strategy shall be developed to guide implementation and compliance to this policy. This policy shall be made available for reference to all members of staff and the county stakeholders upon sensitization.

15.3 Monitoring and Evaluation
This policy shall be monitored and evaluated on continuously to ensure smooth implementation and compliance with legal, regulatory and policy provisions. The Head of ICT Function shall present periodic reports to Senior Management Team (SMT) and County to inform planning, implementation and decision-making.

15.4Review
15.4.1 The policy shall be reviewed every five (5) years. In the event of emergent issues, this Policy shall be reviewed within a period not exceeding two (2) years. Circumstances under which the Policy may be updated and revised include:

15.4.2 Whenever there are changes in the county policies, rules, procedures and guidelines as may be approved from time to time by the County.

15.4.3 Alignment with changes in relevant statutory and regulatory rules and procedures as necessary.

15.4.4 Any proposed changes to the Policy shall be brought to the attention of the Governor and the County for approval and shall be documented and approved