

# COUNTY GOVERNMENT OF NYERI



Town Hall - 2<sup>nd</sup> Floor  
Along Kenyatta Road  
P.O. Box 1112 - 10100  
Telephone 061 2030700  
NYERI

*Email: countysecretary@nyeri.go.ke*

## OFFICE OF THE COUNTY SECRETARY/HEAD OF COUNTY PUBLIC SERVICE

**Our Ref: CGN/CS/EXTRACT/Vol. II/101/416**

**18<sup>th</sup> March, 2026**

**County Executive Committee Member  
Finance, Economic Planning & ICT**

### **MIN CECM 5/16/3/2026: NYERI COUNTY ICT POLICY**

The CECM for Finance, Economic Planning and ICT tabled Nyeri County ICT Policy. He informed Members that the aim of the Policy was to provide a strategic framework guiding the effective adoption, utilization and management of ICT within the County Government of Nyeri, while enhancing governance, service delivery, innovation and socio-economic development.

Cabinet noted that the ICT Policy provides a comprehensive strategic and operational framework to guide how the County Government will deploy, manage and enhance its digital capabilities in order to meet the evolving demands of modern public service delivery and promote sustainable development.

It was subsequently proposed by CECM Fredrick Kinyua and seconded by CECM Esther Muthoni, and resolved **that:**

- i) The Nyeri County ICT Policy be and is hereby adopted. **Action- CECM Finance, Economic Planning and ICT.**

**Certified as true extract of the minutes of the County Executive of County Government of Nyeri duly constituted on 16<sup>th</sup> March, 2026.**

**EDWARD IRUNGU MWANGI  
COUNTY SECRETARY/HEAD OF COUNTY PUBLIC SERVICE**

**Copy to:**

**Chief Officers**

- **Finance & Accounting**
- **Economic Planning & ICT**



**COUNTY GOVERNMENT OF NYERI  
ICT POLICY**

March, 2026





## TABLE OF CONTENT

### Table of Contents

TABLE OF CONTENT.....	i
FOREWORD.....	iv
PREFACE.....	v
ACKNOWLEDGEMENT.....	vi
EXECUTIVE SUMMARY.....	vii
ABBREVIATIONS AND ACRONYMS.....	ix
DEFINITION OF TERMS.....	x
COUNTY OVERVIEW.....	xi
ICT Connectivity.....	xi
CHAPTER ONE: INTRODUCTION.....	1
1.1 ICT Vision, Mission and Core Values.....	1
Vision.....	1
Mission.....	1
Core Values.....	1
1.2 Justification for the policy.....	2
1.3 Scope.....	3
1.4 Policy Statement.....	3
1.5 Policy Objectives.....	3
1.6 Policy Development Process.....	4
1.7 Legal and Institutional Framework.....	5
1.7.1 Legislative and Policy Framework.....	5
1.7.2 Institutional Framework.....	8
CHAPTER TWO: SITUATION ANALYSIS AND THE KEY ISSUES.....	9
2.1 SECURITY.....	9
2.1.1 Network and Data Center Security.....	9
2.1.2 Wireless security.....	9
2.1.3 Public Internet Access.....	9
2.1.4 Cyber and Information Security.....	9
2.2 Secure Desk.....	9
2.3 Encryption and Password Management.....	9
2.3.1 Encryption.....	9

2.3.2 Password Management.....	9
2.4 Access Control.....	10
2.5 Asset Management.....	10
2.6 BYOD.....	10
2.7 Business Continuity and Disaster Recovery.....	11
2.8 Communication.....	11
2.8.1 Social media.....	11
2.8.2 Email.....	11
2.8.3 Website.....	11
2.8.4 Teleconferencing.....	11
2.9 Green ICT and Sustainability.....	12
2.10 ICT Governance.....	12
2.11 ICT Capacity Development.....	13
2.12 Emerging Technologies.....	13
CHAPTER THREE: POLICY FRAMEWORK AND MEASURES.....	14
3.1 Security.....	14
3.1.1 Introduction.....	14
3.1.2 Network and Data Center Security.....	14
3.1.3 Wireless security.....	15
3.1.4 Public Internet Access.....	15
3.1.5 Cyber and Information Security.....	15
3.2 Secure Desk.....	16
3.3 Encryption and Password Management.....	16
3.3.1 Encryption To ensure encryption, the following shall be adhered to;.....	16
3.3.2 Password Management.....	17
3.4 Access Control.....	17
3.5 ICT Asset Management.....	18
3.5.1 Hardware.....	18
3.5.2 Software.....	19
3.5.3 Databases.....	20
3.6 BYOD.....	20
3.7 Business Continuity and Disaster Recovery.....	20
3.7.1 Incident Categories.....	21

3.7.2 Roles and Responsibilities.....	21
3.7.3 Incident Response Process.....	21
3.7.4 Data Backup.....	22
3.8 Communication.....	22
3.8.1 Social Media.....	22
3.8.2 Email.....	22
3.8.3 County Website.....	23
3.8.4 Teleconferencing.....	23
3.9 Green ICT and Sustainability.....	24
3.10 ICT Governance.....	24
3.11 ICT Capacity Development.....	25
3.12 Emerging Technologies.....	25
3.12.1 Cloud Computing.....	25
3.12.2 Artificial Intelligence (AI).....	25
3.12.3 Robotics.....	25
3.12.4 Blockchain.....	25
CHAPTER FOUR: MONITORING, EVALUATION, ACCOUNTABILITY, AND CONTINUED LEARNING.....	26
CHAPTER FIVE: POLICY IMPLEMENTATION.....	27
5.1 Planning and Performance Management.....	27
5.2 Collaboration.....	27
5.3 Staff Capacity Development.....	27
5.4 Establishment of institutions/committees.....	27
5.4.1 ICT Strategy Committee.....	27
5.4.2 ICT Steering Committee.....	28
ANNEXURE ONE: IMPLEMENTATION MATRIX.....	29

---

## FOREWORD

In an era defined by rapid technological advancement, the adoption and integration of Information and Communication Technology (ICT) has become indispensable in driving organizational efficiency, innovation, and socio-economic development. Across the globe, ICT continues to reshape the way governments deliver services, engage citizens, and promote inclusive growth.

Kenya's Vision 2030 recognizes ICT as a key enabler of national development, underscoring its role in transforming public service delivery, enhancing transparency, and fostering innovation. This policy is clearly aligned to the Bottom-up Economic Transformation Agenda (BETA) pillar on Digital Superhighway and Creative Economy. In alignment with the national development goals, the County Government of Nyeri acknowledges the immense potential of ICT in accelerating development and improving the quality of life for its citizens.

The County's Integrated Development Plan (CIDP) emphasizes ICT as a critical driver in fostering youth innovation, wealth creation, and effective service delivery. It is within this framework that the County Government has revised this ICT Policy to guide the structured and strategic application of ICT in governance, resource utilization, and citizen engagement.

This revised policy provides a comprehensive framework for the ethical, professional, and consistent use of ICT across all departments within the County Government. It is designed to align with existing national policies, legal and regulatory frameworks, and to ensure optimal returns on public investments in technology.

The County Government affirms its commitment to the implementation and operationalization of this policy as a tool for enhancing professionalism, accountability, transparency, and innovation in public service. We further recognize the pivotal role ICT plays in building a digitally empowered society and reaffirm our support for its adoption in improving service delivery and fostering inclusive development for all residents of Nyeri County.

It is our expectation that this policy will serve as a living document, responsive to emerging technologies and evolving public needs, and that it will guide the County Government towards full realization of the Kenya Digital Economy Blueprint.

**H.E. Dr. Mwalimu Mutahi Kahiga, PhD, EGH**  
Governor, County Government of Nyeri.

## PREFACE

This is the second ICT policy to be prepared by the County Government of Nyeri since the inception of devolution. It is a revision of the ICT Policy 2021 which was driven by the need to align the county with the rapid technological advancements. This review aims to adopt emerging technologies to strengthen governance, enhance service delivery, and foster innovation. By integrating Cloud Computing, Artificial Intelligence, Robotics, and Blockchain technology, the policy seeks to improve scalability, data accessibility, automation, transparency, and disaster recovery, ensuring a more efficient and responsive government framework.

The revision of the ICT Policy marks a significant milestone in the County Government of Nyeri's commitment to leveraging technology as a strategic tool for development, improved governance, and enhanced service delivery.

In today's digital era, the effective use of Information and Communication Technology (ICT) is central to the transformation of public service. It enables efficiency, transparency, innovation, and timely access to information and services. Recognizing this, the County Government has prioritized ICT as a key pillar in achieving its development goals, in alignment with Kenya's Vision 2030 and the Kenya Digital Economy Blueprint.

This policy provides a structured framework to guide the planning, implementation, management, and evaluation of ICT initiatives within the County. It aims to standardize ICT practices, ensure effective utilization of resources, and create a secure and reliable digital environment that supports both internal operations and citizen-focused services.

The development of this policy has been informed by wide consultations, benchmarking with county and national best practices, and an in-depth understanding of the County's specific needs and aspirations. It outlines the principles, objectives, and strategic areas that will guide ICT adoption and integration across all departments of the County Government.

As technology continues to evolve, so too must the County's approach to managing and deploying ICT. This policy is therefore set to be reviewed every three (3) years or as per need arises to remain relevant, responsive, and aligned with emerging trends and legislative changes.

We invite all stakeholders—both internal and external—to embrace the principles outlined herein and to support the implementation of this policy for the collective benefit of Nyeri County and its residents.

**Robert Thuo Mwangi,**  
County Executive Committee Member,  
Finance, Economic Planning and ICT,  
County Government of Nyeri.

---

## ACKNOWLEDGEMENT

The development of the County Government of Nyeri's ICT Policy has been a collaborative and consultative effort involving various stakeholders whose contributions were invaluable in shaping this important document.

We wish to acknowledge the unwavering support and visionary leadership of **H.E. the Governor of Nyeri County**, whose commitment to digital transformation continues to steer the County toward innovation-driven service delivery and economic growth. I also wish to thank the entire County Executive Committee for their critical input in the development of this policy.

Special appreciation goes to the CECM Finance, Economic Planning and ICT and Chief Officer for Finance, Accounting and ICT, for their guidance, technical insight, and coordination throughout the policy development process. We also extend our gratitude to the members of the ICT technical team, the Office of the County Attorney, and county staff whose input and experiences enriched the content and relevance of this policy.

We are particularly grateful to the ICT Authority for providing technical assistance and expert advice. Your contributions played a crucial role in aligning this policy with national strategies and global best practices.

Lastly, we thank all stakeholders - both within government and the broader community - who participated in consultations, shared feedback, and demonstrated a strong commitment to building a digitally empowered Nyeri County.

This policy reflects our shared vision, and we look forward to its successful implementation for the benefit of all.

**Edward Irungu Mwangi,**  
County Secretary,  
County Government of Nyeri.

---

## EXECUTIVE SUMMARY

The Nyeri County ICT Policy sets out a strategic and operational roadmap for how the County Government will deploy, govern, and grow its digital capabilities to meet the demands of modern public service and sustainable development.

This policy begins by establishing a strong foundational case for ICT as a key pillar in the transformation of County operations, aligning with Kenya’s Vision 2030, the Kenya Digital Economy Blueprint, and the County Government’s development plans. It articulates the County Government’s vision for ICT-led innovation, inclusive access, and improved service delivery, grounded in principles of integrity, transparency, professionalism, security, and citizen participation.

A comprehensive situation analysis outlines the County’s current ICT environment—including infrastructure, risks, capacity gaps, and opportunities. It identifies key vulnerabilities in systems, cybersecurity, asset management, and disaster recovery mechanisms, while also highlighting opportunities in public internet access, integrated services, and cloud computing.

The policy responds to these challenges by setting out detailed strategies in several core areas:

**Cybersecurity & Data Protection:** It establishes clear standards for network security, information classification, encryption, access control, password management, and physical security—ensuring confidentiality, integrity, and availability of County data and systems.

**ICT Asset & Software Management:** The policy defines the lifecycle management of all ICT hardware, software, databases, and digital platforms, with clear guidelines on procurement, usage, tagging, disposal, and licensing compliance.

**Communication & Digital Engagement:** It introduces policy direction for web, social media, and email governance—ensuring that all communication is timely, secure, and aligned with the County Government’s values, while also protecting official systems from misuse or compromise.

**Business Continuity & Disaster Recovery:** Recognizing the County’s increasing reliance on digital systems, the policy includes a framework for data backup, risk mitigation, redundancy planning, and response protocols for ICT-related incidents or disruptions.

**Green ICT & Sustainability:** Environmental stewardship is woven into the policy through the promotion of energy-efficient technologies, e-waste reduction, virtualization, and sustainable procurement practices in line with global green ICT standards.

**ICT Governance:** The policy strengthens institutional frameworks and leadership structures, promotes interdepartmental coordination, and ensures compliance with relevant legal and regulatory frameworks, including data protection, procurement, and ethics.

---

**Capacity Development:** It prioritizes digital literacy across departments, professional development of ICT staff, and formal collaboration with academic institutions and innovation hubs to build a digitally competent workforce.

**Emerging Technologies:** The County positions itself for the future by establishing principles and action plans for piloting and adopting innovations such as artificial intelligence, robotics, blockchain, and cloud computing—with ethical and regulatory guardrails.

**Monitoring, Evaluation, and Learning:** A dedicated chapter sets out how implementation progress will be tracked, reviewed, and improved over time—ensuring that the policy evolves in step with technology and public expectations.

**Implementation Framework:** Finally, the policy outlines how it will be embedded into the County Government’s operations through structured planning, budgeting, institutional roles, and integration with the CIDP and other development plans.

Overall, this ICT Policy provides a unified, forward-looking approach to digitizing the County Government of Nyeri. It is not just a technology framework—it is a governance tool, a security standard, a service improvement plan, and a social inclusion strategy. It will serve as a living document—adaptable to change, responsive to innovation, and firmly rooted in the County Government’s commitment to efficient, transparent, and people-driven governance.

## ABBREVIATIONS AND ACRONYMS

<b>AES</b>	Advanced Encryption Standard
<b>BC/DR</b>	Business Continuity and Disaster Recovery
<b>BETA</b>	Bottom-up Economic Transformation Agenda
<b>BPO</b>	Business Process Outsourcing
<b>BYOD</b>	Bring Your Own Device
<b>CAPA</b>	Corrective and Preventative Action
<b>CCTV</b>	Closed Circuit Television
<b>CECM</b>	County Executive Committee Member
<b>CGN</b>	County Government of Nyeri
<b>CRA</b>	Commission on Revenue Allocation
<b>DICT</b>	Directorate of ICT
<b>EAL4</b>	Evaluation Assurance Level 4
<b>E-Waste</b>	Electronic Waste
<b>ICT</b>	Information and Communication Technology
<b>ICTA</b>	Information Communication Technology Authority
<b>IDS</b>	Intrusion Detection Systems
<b>IP</b>	Internet Protocol
<b>IPS</b>	Intrusion Prevention Systems
<b>IT</b>	Information Technology
<b>ITS</b>	Integrated Telephony Systems
<b>LAN</b>	Local Area Network
<b>MEAL</b>	Monitoring, Evaluation, Accountability, and Learning
<b>MICDE</b>	Ministry of Information Communication and the Digital Economy
<b>OAG</b>	Office of the Auditor General
<b>OCOB</b>	Office of the Controller of Budget
<b>ODPC</b>	Office of the Data Protection Commissioner
<b>OEM</b>	Original Equipment Manufacturer
<b>PC</b>	Personal Computer
<b>PII</b>	Personal Identifiable Information
<b>PIN</b>	Personal Identification Number
<b>RSA</b>	Rivest-Shamir-Adleman Encryption
<b>BPO</b>	Business Process Outsourcing
<b>SaaS</b>	Software as a Service
<b>SDGs</b>	Sustainable Development Goals
<b>SD-WAN</b>	Software Defined Wide Area Network
<b>VPN</b>	Virtual Private Network

---

## DEFINITION OF TERMS

- **Personal Identifiable Information (PII):** Information that can identify an individual, such as names, addresses, and other private details (e.g., staff and payroll spreadsheets).
- **Sensitive Personal Data:** A more critical category that includes details about an individual's health, ethnic origin, religious beliefs, criminal convictions, etc., requiring even more stringent security measures.
- **Corporately and Commercially Sensitive Information:** Data whose improper disclosure could harm the organization's competitiveness or legal standing, such as building leases, contracts, or internal plans.
- **Encryption:** is the process of converting information into a code (readable), making it unreadable to unauthorized individuals.
- **Password Management:** This refers to the practices and tools used to securely store, organize, and control access to passwords by creating strong, unique passwords, storing them safely, and ensuring convenient access when needed, balancing security and usability.
- **Incident:** Any event that disrupts normal ICT operations, including cyberattacks, system failures, data breaches, or natural disasters.
- **Critical Incident:** An event causing major disruption to core business functions.
- **Minor Incident:** An event with limited impact, easily contained and resolved.
- **Data Center:** A dedicated space within a building, used to house computer systems and associated components, such as telecommunications and storage systems.
- **Cyber Security:** This refers to any aspect that protects an organization's employees, data, network and systems from cyber-attacks that are aimed at unauthorized access, changing, stealing or destroying sensitive information
- **Director:** Means the director incharge of ICT
- **Secure Desk:** the practice of implementing a Clean Desk Policy, where employees ensure that sensitive and confidential physical and digital information is not left unsecured in their workstations at the end of the day, or when left unattended

---

## COUNTY OVERVIEW

Nyeri County has an estimated population of 828,805 persons consisting of 49 percent male and 51 percent female according to the projections by KNBS, 2022. Most of the inhabitants of the County are from the Kikuyu community who are predominantly farmers growing tea and coffee as cash crops. They also engage in subsistence farming of crops such as maize, beans, assorted vegetables, and sweet potatoes as well as small scale livestock farming. Other communities living in the county include Luo, Meru, Kamba, Embu, Borana, Somali and virtually all Kenyan communities who are mostly engaged in own businesses or employed by the government.

Nyeri County is one of the 47 counties in Kenya and is located in the central region of the country with its headquarter located in Nyeri Town. It covers an area of 3,325 Km<sup>2</sup> and is situated between longitudes 36°38' east and 37°20' east and between the equator and latitude 0°38' south. It borders Laikipia County to the north, Kirinyaga County to the east, Murang'a County to the south, Nyandarua County to the west and Meru County to the northeast.

The county is easily accessible by road from Nairobi and the neighboring counties. It takes about two hours travel to Nyeri from Nairobi (approximately 150km), two hours from Nakuru (approximately 167km), 45 minutes from Nanyuki (approximately 60km) and one and a half hours from Nyahururu (approximately 100km). There is no regular transport by air to Nyeri although there are three airstrips namely Mweiga on the Nyeri-Nyahururu highway, Nyaribo on the Nyeri-Nanyuki road about 15km from Nyeri town and the Nanyuki air strip near Nanyuki Town.

### **ICT Connectivity**

Nyeri County has made significant progress in digital infrastructure through projects like the National Optic Fiber Backbone Infrastructure (NOFBI), which connects key sites, alongside the Digital Superhighway Project that boosts fast internet access in schools, health centers, and Wi-Fi spots. The Last Mile County Connectivity Project (LMCCP) links government offices, hospitals, and police stations, while public Wi-Fi hotspots, including free access at Nyeri Open Market since 2022, help local traders go online. Internet use in the county now stands at 50.1%, up from about 22.7% in 2019, according to the 2023-2024 Kenya Housing Survey. Computer use is at 21.3%, ranking second highest in Kenya. These efforts support digital hubs that build tech skills, spark new ideas, and create jobs, with Nyeri hosting BPO centers like Jitu and OnQ Kenya.

---

## CHAPTER ONE: INTRODUCTION

This Chapter contains policy statements on Information and Communication Technology (ICT) services and Information Systems that are of strategic importance to the County Government.

### 1.1 ICT Vision, Mission and Core Values

#### Vision

To be a digitally empowered County that delivers innovative, secure, and inclusive ICT-driven services.

#### Mission

To transform public service delivery and governance in Nyeri County through strategic adoption of technology, promotion of digital skills, secure information management, and citizen-focused digital innovation.

#### Core Values

**Digital Integrity:** We uphold ethical standards in the use, management, and dissemination of digital resources and data; ensuring privacy, security, and transparency in all ICT operations.

**Innovation:** We aim to foster a culture of continuous improvement, creativity, and technological advancement to solve public service challenges and improve lives.

**Accountability:** We are committed to responsible ICT governance, prudent use of resources, and measurable outcomes in all our initiatives.

**Inclusivity:** We strive to bridge the digital divide by ensuring all residents—including youth, women, persons with disabilities, and marginalized groups can access and benefit from digital services.

**Professionalism:** We promote technical competence, ethical conduct, and service excellence among all ICT personnel and County staff.

**Sustainability:** We integrate environmental responsibility into ICT planning and operations, embracing green technologies and energy-efficient practices.

**Collaboration and teamwork:** We value partnerships with stakeholders and peers such as government agencies, the private sector, academia, and citizens to co-create meaningful and lasting digital solutions.

**Resilience:** We commit to building robust, secure, and adaptable systems that ensure continuity of services and protection of digital infrastructure in the face of evolving risks.

**Agility:** We commit to ensure that our strategies, regulations and digital services remain responsive and adaptive in the face of rapid technological and societal changes.

## **1.2 Justification for the policy**

The development of the ICT Policy for the County Government of Nyeri is informed by the growing importance of Information and Communication Technology (ICT) in enabling efficient, transparent, and responsive governance. As the world increasingly embraces digital solutions, it is imperative that county governments establish structured, secure, and inclusive frameworks to guide ICT adoption and application.

Several key factors justify the need for this policy:

### **1. Alignment with National Development Goals**

Kenya's Vision 2030, National ICT Master Plan and the Kenya Digital Economy Blueprint, Bottom-Up Economic Transformation Agenda (BETA) identify ICT as a key enabler of national transformation. For Nyeri County to contribute meaningfully to these national goals, a localized policy is necessary to guide ICT planning, investment, and implementation within the county context.

### **2. Improved Service Delivery**

ICT provides tools for automating services, streamlining operations, enhancing communication, and improving citizen access to information and government services. This policy will help institutionalize ICT use in public service to ensure efficiency, quality, and consistency in delivery.

### **3. Need for a Coordinated ICT Framework**

Without a policy, ICT initiatives may be fragmented, duplicative, or misaligned. This policy provides a unified and coordinated framework that ensures all ICT projects and systems within the County Government are interoperable, scalable, cost-effective, and aligned with strategic priorities.

### **4. Security and Data Protection**

As the County Government increasingly digitizes its operations, it must address risks related to data privacy, cybersecurity, and system resilience. This policy sets standards and guidelines to ensure secure handling and protection of information assets and associated hardware.

### **5. Capacity Building and Digital Inclusion**

This policy is an essential guide on training, skill development, and empowerment of county staff, as well as the digital inclusion of youth, women, persons with disabilities, and marginalized groups. It supports the creation of opportunities for innovation and entrepreneurship through technology.

### **6. Accountability and Resource Optimization**

Public investment in ICT must yield measurable value. This policy promotes good governance, transparency, and accountability in the acquisition, deployment, and use of ICT resources within the County Government.

## 7. Emerging Technologies and Innovation

The dynamic nature of technology requires a forward-looking policy to guide the adoption of emerging innovations such as artificial intelligence, big data, cloud computing, and mobile platforms. This ensures that Nyeri County remains adaptive and competitive in a digital economy.

In conclusion, this policy is not only a strategic necessity but also a foundational instrument for transforming Nyeri County into a smart, citizen-focused, and future-ready.

### 1.3 Scope

This policy applies to all users of the CGN ICT resources who are required to agree to, and abide by, its terms.

### 1.4 Policy Statement

The purpose of this Policy is to establish a comprehensive framework that guides the planning, implementation, use, management, and governance of ICT within the CGN.

The County Government shall:

- Ensure that ICT is integrated into all aspects of governance and public service;
- Promote professionalism, accountability, transparency, and ethical use of ICT by all public officers;
- Provide secure, reliable, inclusive digital services and resilient systems to the county residents;
- Support innovation, particularly among youth, through digital platforms and opportunities;
- Align all ICT investments and initiatives with county and national laws, policies, and regulatory standards;
- Foster partnerships with stakeholders to expand access, build capacity, and sustain innovation.

Through this commitment, CGN endeavors to position itself as a model of digital transformation and innovation within the public sector, ultimately improving the lives of the county residents and contributing to national development goals.

### 1.5 Policy Objectives

To provide a strategic framework that guides the effective adoption, utilization, and management of ICT within the County Government of Nyeri, with the aim of enhancing governance, service delivery, innovation, and socio-economic development. The specific objectives are to:

- Adopt emerging technologies and industry trends to enhance efficiency in delivery of the County Government of Nyeri's core mandate;
- Promote innovation and digital inclusion, especially among youth and marginalized groups;
- Ensure data security, privacy, and continuity of digital services;

- Enhance stakeholder collaboration;
- Encourage ethical, responsible, and professional use of ICT;
- Adopt relevant legal, regulatory, and policy frameworks at both county and national levels.

### 1.6 Policy Development Process

In line with the Constitutional principles of participatory policy making and review, this policy was developed through a consultative process where key stakeholders were mapped and engaged as summarized in the table below.

		INTERESTS	
		HIGH	LOW
POWER/ INFLUENCE	HIGH	<ul style="list-style-type: none"> <li>● Development Partners;</li> <li>● ODPC;</li> <li>● CGN (Executive &amp; Assembly);</li> <li>● National Treasury.</li> </ul>	<ul style="list-style-type: none"> <li>● OAG;</li> <li>● ICTA;</li> <li>● MICDE;</li> <li>● OCOB;</li> <li>● CRA.</li> </ul>
	LOW	<ul style="list-style-type: none"> <li>● Citizens;</li> <li>● Special groups;</li> <li>● Academia;</li> <li>● Research Organizations;</li> <li>● Private Sector;</li> <li>● Civil Society Organizations;</li> <li>● Professional Bodies.</li> </ul>	Other County Governments.

## **1.7 Legal and Institutional Framework**

This policy is informed by the following legal and institutional framework;

### **1.7.1 Legislative and Policy Framework**

#### **1.7.1.1: Constitution of Kenya, 2010**

Article 10 provides for good governance, integrity, transparency and accountability

Article 31 guarantees every person's right to privacy, which includes the right not to have the privacy of their communications infringed.

Article 35 guarantees the right to access to information held by the state and imposes on the latter the need to publish and publicize any information affecting the nation.

Article 232 outlines the core values and principles of public service, mandating high standards of professional ethics, efficient resource use, public involvement in policymaking, accountability for administrative acts, and transparency in government.

#### **1.7.1.2 The County Governments Act, 2012**

In addressing modalities for citizen participation, Section 91 of the Act, requires county governments to facilitate the establishment of structures for citizen participation including ICT-based platforms.

Section 95 (1) provides that a county government shall establish mechanisms to facilitate public communication and access to information in the form of media with the widest public outreach in the county, which may include ICT centres. The CIDP 2023-2027 has outlined modalities for installing ICT hubs across the sub counties.

Section 117 provides for the standards and norms of public service; subsection (2) (c) and (d) provide that public services shall be equitably delivered in a manner that accords to the appropriate incorporation of the use of ICT and financial sustainability.

#### **1.7.1.3 The Environmental Management and Co-ordination Act, 1999**

The Act prohibits dangerous handling and disposal of waste in such a way as to cause pollution to the environment and ill health to any person. It prescribes the manner in which e-waste and such other hazardous waste shall be handled and/or disposed.

#### **1.7.1.4 The Data Protection Act, 2019**

The Act gives effect to Article 31 (c) and (d) of the Constitution of Kenya; establishes the ODPC and makes provisions for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors.

Section 25 provides for principles of data protection, which include a requirement for data controllers/processors to ensure that personal data is collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes.

Section 26 guarantees a data subject the right to be informed of the use to which their personal data is to be put; this personal data shall be collected directly from the data subject by the data controller or processor and the latter(s) has a duty to notify the data subject of such collection.

#### **1.7.1.5 The Public Procurement and Asset Disposal Act, 2015**

The Act gives effect to Article 227 of the Constitution; to provide procedures for efficient public procurement and for asset disposal by public entities.

Section 165 (2) provides that radioactive or electronic waste shall be disposed of only to persons licensed to handle the respective waste under section 88 of the Environmental Management and Co-ordination Act (Cap. 387).

#### **1.7.1.6 The Computer Misuse and Cybercrimes Act, 2018**

The Act was established to provide for offences relating to computer systems; and to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes, among others.

Part III provides for offences, which include unauthorised access, unauthorised interference to a computer system, program or data, unauthorised disclosure of password or access codes, cyber espionage, computer fraud, cyber harassment, among others.

#### **1.7.1.7 The Access to Information Act, 2016**

The Act gives effect to Article 35 of the Constitution of Kenya and mandates public entities to facilitate access to information held by themselves. It provides a framework for public entities to proactively disclose information that they hold and to provide information on request in line with the constitutional principles; further, it promotes routine and systematic information disclosure by public entities on constitutional principles relating to accountability, transparency and public participation and access to information.

While disseminating such information, public entities are expected to take into consideration the need to reach persons with disabilities, the cost, local language and the most effective method of communication in that local area; the information shall be made easily accessible and available free or at cost taking into account the medium used, which includes the internet or electronic form.

#### **1.7.1.8 The National ICT Policy, 2019**

The Policy poses itself as a facilitator for the creation of infrastructure and frameworks that support the growth of data centres, pervasive instrumentation (Internet of Things), machine learning and local manufacturing while fostering a secure, innovation ecosystem; to grow the GDP through the use of ICT, among other things.

The Policy focuses on four (4) key areas namely, Mobile First, Market, Skills & Innovation, and Public Service Delivery; where the government envisions the availability/accessibility of its services online. The Policy calls for all arms of government to build, deploy, operate and manage locally built back-end and front-end systems to deliver services.

### **1.7.1.9 The Kenya National ICT Master Plan 2022-2032**

This 10-year plan forms a reference point for all government ICT plans. It builds on the pillars of the Kenya Digital Economy Blueprint. The Plan aims to provide a holistic and coordinated approach so as to ensure the alignment and optimization of ICT's resources with ever changing needs; with the intention to enable effective and efficient implementation of government ICT initiatives, strategies and guide policy direction of the country. It also envisions the streamlining of ICT projects across government, ensure inter-operability of systems by eliminating technology silos, providing for the sharing and re-use of viable ICT assets, guaranteeing privacy and data protection and providing assurance on cyber security.

### **1.7.1.10 The National Environment Policy, 2013**

The policy provides a governance framework for environmental management. It imposes the need to manage the inherent risks at production, use, transport and waste disposal, among others in an environmentally sound manner. It calls for the establishment of appropriate disposal facilities for toxic and hazardous substances.

### **1.7.1.11 Kenya Vision 2030**

The Kenya Vision 2030 lays the foundation for social and economic development in Kenya and recognises ICT as an enabler. It aims to enhance digital literacy, foster innovation, promote local ICT software development and expand access to broadband. It also aims to make government services more accessible and efficient through online platforms.

### **1.7.1.12 The Bottom-Up Economic Transformation Agenda (BETA)**

This Agenda is implemented by the Fourth Medium Term Plan (MTP IV) 2023-2027 and is geared towards economic turnaround and inclusive growth through a value chain approach. The fifth pillar of the BETA agenda is Digital Superhighway and Creative Economy, where the government intends to leverage on technology and creative industries for economic growth and job creation.

### **1.7.1.13 The Kenya Digital Economy Blueprint**

The Blueprint seeks to provide a conceptual framework adopted by Kenya in its quest towards the realization of a successful and sustainable digital economy. It identifies the five pillars of the digital economy that are described as Digital Government, Digital Business, Infrastructure, Innovation-Driven Entrepreneurship and Digital Skills and Values.

### **1.7.1.14 Other policies and laws with implications on ICT Management**

- a) **The Industrial Property Act**; which provides for the promotion of inventive and innovative activities, to facilitate the acquisition of technology through the grant and regulation of patents, utility models, technovations and industrial designs, among others; and which will guide in management of ICT innovations and/or intellectual property.
- b) **The Persons With Disabilities Act**

While enforcing the right to equality and non-discrimination, the Act provides for putting in place specific measures including support services which are necessary to accelerate or achieve equality and eliminate discrimination against persons with disability. The Directorate shall consult widely with the NCPWD, the Kenya National Association of the Deaf, the National Society for the Blind, among other special groups to ensure accessibility to platforms for both employees and members of the public while rendering and receiving public services respectively.

- c) **The Anti-corruption and Economic Crimes Act**; which provides for prevention, investigation and punishment of corruption, economic crime and related offences, some of which are referenced in this Policy.
- d) **The Energy Act**; which provides for renewable energy and posits the county government in implementing national government policies relating to the same. The county commits to adopt practices that uphold the Constitutional principle of sustainability.
- e) **The Conflict of Interest Act, 2025**; which provides for the management and regulation of conflict of interest.
- f) **The Public Archives and Documentation Services Act**; which provides for the preservation of public archives and public records.
- g) **The Kenya Artificial Intelligence Strategy, 2025 - 2030**; which provides a framework to guide Kenya in harnessing the power of AI and safeguarding national interests by embedding robust data sovereignty, a cybersecurity framework, and ethical oversight in AI deployment.
- h) **The 2030 Agenda for Sustainable Development**; which provides for the seventeen (17) Sustainable Development Goals (SDGs) among which include **Goal 9**:

## **1.7.2 Institutional Framework**

In exercise of its mandate, the DICT collaborates with the following institutions.

### **1.7.2.1 Information Communication and Technology Authority (ICTA)**

Established by Legal Notice No. 183 of 16<sup>th</sup> August 2013, the Authority's functions include setting and enforcing ICT standards and guidelines for public service delivery, promoting e-government, ICT literacy and capacity, and supervising the design, development and implementation of critical ICT projects across the public service, among others.

### **1.7.2.2 Office of the Data Protection Commissioner**

Established by the Data Protection Act, 2019 the Office of the Data Protection Commissioner's functions include exercising oversight on data processing operations, either of own motion or at the request of a data subject, and verifying whether the processing of data is done in accordance with its enabling Act; and carrying out inspections of public entities with a view to evaluating the processing of personal data.

### **1.7.2.3 Communications Authority of Kenya (CA)**

---

Established by the Kenya Information and Communications Act, 1998, CA is the regulatory authority for the communications sector in Kenya and is responsible for facilitating their development.

---

## **CHAPTER TWO: SITUATION ANALYSIS AND THE KEY ISSUES**

### **2.1 SECURITY**

#### **2.1.1 Network and Data Center Security**

The foundation of the county's ICT structure is the Data and Communications Network which is facilitated and supported by components consisting of wired and wireless networks, and supporting systems installed throughout the County Government's various buildings and offices across the county. This also includes institutions and facilities where the county provides free public internet access.

The County Government relies heavily on its Data and Communications Network infrastructure to:

- a) Carry out its business functions and activities using connected IT systems
- b) Communicate via Integrated Telephony Systems (ITS)
- c) Facilitate Video Conferencing Technologies
- d) Provide wireless —Hot Spot access zones and ICT connected services to the public

#### **2.1.2 Wireless security**

The wireless network must meet high standard levels of security guided by security policies. This is to ensure that the deployment of wireless networking is controlled and managed in a centralized way.

#### **2.1.3 Public Internet Access**

When providing public internet access facilities, CGN recognizes its obligation to protect public and County Government information, equipment and systems from threats.

#### **2.1.4 Cyber and Information Security**

Cyber security refers to any aspect that protects an organization's employees, data, network and systems from cyber-attacks that are aimed at unauthorized access, changing, stealing or destroying sensitive information. With the ever-changing technology world, cybercrimes have been on the rise.

### **2.2 Secure Desk**

This is a component of a larger ICT Security Policy designed to protect the confidentiality, integrity, and availability of an organization's information assets. It focuses specifically on securing information, whether in physical or electronic form, when it is not in use or when a workstation is unattended.

### **2.3 Encryption and Password Management**

#### **2.3.1 Encryption.**

Encryption is crucial for protecting sensitive data during storage and transmission. With the ever-increasing demand on the use of ICT systems across the CGN, the protection of electronic information and access to storage systems is vital to ensure data security, data integrity, confidentiality, privacy and compliance.

#### **2.3.2 Password Management**

With continuing reliance on ICT systems, it has become increasingly important to ensure that the integrity of all systems and access passwords used across CGN is maintained.

---

## **2.4 Access Control**

While the county is committed to providing public access to its systems and information (availability), it is equally vital to protect sensitive data from unauthorized disclosure (confidentiality) and ensure its accuracy (integrity).

## **2.5 Asset Management**

CGN has made commendable progress in integrating ICT into public service delivery. This has resulted in increased acquisition and use of key ICT assets, namely hardware, software, databases, and user-owned devices (BYOD). However, the rapid expansion of these assets across departments has exposed gaps in standardization, tracking, and accountability.

In terms of hardware, the county has experienced challenges in ensuring consistent coordination during acquisition processes. Departments often procure equipment independently without adequate technical input from the DICT, resulting in compatibility issues and lack of standardization. Furthermore, asset tagging, inventory management, and proper storage of equipment are inconsistently enforced. There are cases of equipment being left unattended, stored improperly, or moved between offices without formal authorization or documentation. Repairs and modifications are sometimes undertaken without ICT oversight, compromising asset tracking and lifecycle records.

With regard to software, there is no formalized approach to documenting ownership of developed or acquired software, including associated source codes and licenses. In many instances, software is deployed without clear records of who owns, maintains, or supports it. Additionally, software sourced for County operations is not always fully handed over with the required access credentials, licenses, or supporting materials, making it difficult to manage or sustain after initial deployment.

Databases are core to the county's information systems, yet there is no centralized and updated register documenting their existence, purpose, or custodianship. Many databases are managed in isolation, without clear identification of business owners or ICT administrators responsible for their upkeep. Change control processes—such as version updates, structural modifications, or platform migrations—are often informal and undocumented, leading to difficulties during audits or in the event of data integrity issues.

## **2.6 BYOD**

The adoption of BYOD practices has improved mobility and flexibility among staff. However, there are no formal procedures for registering or tracking user-owned devices used for official work. This lack of documentation complicates accountability, especially when devices are brought into county premises or used to access county systems. Additionally, expectations regarding user responsibilities for device maintenance, updates, and secure use are not clearly communicated or enforced.

---

## **2.7 Business Continuity and Disaster Recovery**

As county governments increasingly rely on digital systems to deliver essential services—ranging from health records and revenue collection, to land management and citizen engagement—the need for robust BC/DR frameworks has become critical. Disruptions caused by cyberattacks, system failures, natural disasters, or human error can severely impact service delivery, public trust, and operational efficiency.

Despite the growing digital footprint, the CGN lacks a formal BC/DR strategy. While the county recognizes the importance of IT service continuity, existing frameworks are often too complex or costly to implement, leaving the county vulnerable to prolonged outages and data loss.

The county faces several critical challenges in BC/DR, including fragmented systems, absence of formal tested recovery plans and inadequate power and data infrastructure. Lack of testing or simulation exercises exposes the county to prolonged service disruptions and data loss during crises. These challenges are further exacerbated by budget constraints.

## **2.8 Communication**

### **2.8.1 Social media**

Social media platforms offer the County Government dynamic channels to engage directly with citizens, share timely information, and foster community participation. The CGN uses platforms like YouTube, Facebook, and X or any other approved platform to disseminate information.

### **2.8.2 Email**

CGN recognizes email as a critical tool for official communication, facilitating efficient interaction among employees, vendors, and agents.

### **2.8.3 Website**

CGN's official website, [www.nyeri.go.ke](http://www.nyeri.go.ke), plays a key role in sharing information and delivering services to the public. As the demand for timely and accurate updates grows, clear policies on content submission and approval are essential to maintain consistency, accountability, and public trust in the platform.

### **2.8.4 Teleconferencing**

The county has a relatively stable internet that has supported several virtual meetings especially post Covid-19 period.

---

## **2.9 Green ICT and Sustainability**

CGN is committed to promoting environmentally sustainable practices in all ICT operations and investments. The county's development agenda, as outlined in its Integrated Development Plan (CIDP 2023–2027), emphasizes environmental protection, innovation, and the use of ICT to enhance service delivery.

Currently, CGN's ICT infrastructure is expanding, but much of it relies on energy-intensive systems and hardware, contributing to increased carbon emissions and electronic waste. Paper-based processes remain prevalent in many departments, and the use of non-renewable energy sources in ICT operations further exacerbates environmental impact.

Despite these challenges, there are significant opportunities to adopt energy-efficient technologies, transition to cloud-based systems, and implement e-waste recycling programs. The county also has the potential to leverage solar-powered ICT. However, institutional capacity to implement and monitor green ICT initiatives is limited, and awareness among staff and citizens about sustainable ICT practices remains low.

Public participation forums and youth engagement platforms have proven effective in shaping development priorities, and these can be harnessed to co-create and promote green ICT solutions. National policies on climate change, ICT, and environmental protection provide a supportive framework, but enforcement and integration at the county level need strengthening. By aligning with the SDGs and BETA, CGN has a unique opportunity to lead in green innovation and digital sustainability.

## **2.10 ICT Governance**

CGN recognizes ICT as a strategic enabler for service delivery, economic growth, and citizen engagement, in alignment with Kenya's Vision 2030 and the Digital Economy Blueprint, while existing ICT governance structures are in place they require strengthening to ensure consistent policy enforcement, cross-departmental coordination, and strategic oversight.

CGN has made progress in developing organizational-wide ICT systems, yet challenges persist in system interoperability, data sharing, and integration across departments due to limited ICT infrastructure in rural areas and uneven digital literacy among staff and citizens hindering equitable access to digital services.

Cybersecurity and data protection remain key issues in the CGN which is greatly influenced by the Human resource capacity in ICT which remains insufficient, with a need for continuous training, recruitment, and retention of skilled personnel.

Citizen-facing digital platforms are emerging, but adoption and utilization remain low due to limited awareness and accessibility.

---

Whereas the county’s ICT policy framework emphasizes professionalism, ethical use, and accountability, monitoring and evaluation mechanisms are not yet fully institutionalized.

## **2.11 ICT Capacity Development**

CGN has made notable strides in embracing ICT to enhance service delivery, governance, and citizen engagement. With initiatives such as automated revenue collection, digital land records, and e-health systems, the county is aligning itself with Kenya’s Vision 2030 and the Digital Economy Blueprint. However, the success and sustainability of these digital transformations depend heavily on the capacity of county personnel to manage, innovate, and adapt to evolving technologies.

ICT capacity development is not merely about technical training—it encompasses strategic planning, digital literacy, change management, and institutional readiness. Despite growing demand for digital services, CGN faces persistent challenges in building and maintaining a skilled ICT workforce across departments.

## **2.12 Emerging Technologies**

Emerging technologies are revolutionizing how governments deliver services, engage citizens, and manage resources. CGN recognizes the transformative potential of innovations such as **Cloud Computing**, **Artificial Intelligence (AI)**, **Blockchain** and **Robotics** in achieving its development goals.

---

## CHAPTER THREE: POLICY FRAMEWORK AND MEASURES

### 3.1 Security

#### 3.1.1 Introduction

The County Government has identified the aspects below to enable implementation of robust policies to protect the confidentiality, integrity, and availability of both physical and digital assets.

- a. Network and data center security
- b. Secure Desk
- c. Encryption and Password management
- d. Access control

#### 3.1.2 Network and Data Center Security

To ensure network and data center security, the following shall be adhered to;

- a. Authorized visitor(s)/contractors to the data center shall be issued with a county government visitors badge, signed in/out in the data center register and accompanied by an authorized ICT officer at all times;
- b. Cleaner(s) shall be accompanied by an authorized ICT officer;
- c. Access to and knowledge of data center access codes are restricted to the director or an authorized ICT officer;
- d. Data center doors shall always be kept locked;
- e. Food and beverages are prohibited in the data center;
- f. All network equipment security updates shall be up-to-date at all times;
- g. All unnecessary services running on network devices shall be disabled;
- h. Logical separation of the network shall be implemented;
- i. All security devices deployed shall be EAL4 compliant;
- j. Data center equipment and cables shall be properly labelled;
- k. Network configurations shall not be circulated outside the Network team;
- l. New network equipment shall be compatible with the existing ICT infrastructure;
- m. Configuration changes by a contractor to the network devices shall be authorized by the director;
- n. Equipment failure/planned maintenance shall be communicated to affected users, clearly indicating the estimated downtime;
- o. Servers shall be regularly updated with the latest Operating System security updates and patches;
- p. Servers shall be protected from malicious software and viruses using industry standard antivirus;
- q. Servers shall maintain a record of all event logs;
- r. Backup & restore procedures and routines shall be employed so that systems and data files can be restored and recovered in the quickest, most efficient time possible;
- s. Disaster recovery procedures shall be in place in the event of loss of Server(s) or IT infrastructure and procedural documentation must be regularly updated.

### **3.1.3 Wireless security**

To ensure wireless security, the following shall be adhered to;

- a. All Wireless LANs shall be monitored and maintained by the DICT;
- b. Installation of any non-standard wireless access points is prohibited and only wireless network equipment authorized by the ICT directorate shall be permitted on any CGN's network;
- c. Wireless technology shall be compliant with the 802.11 standards;
- d. All wireless access points used by staff on the county government's secure wireless network shall conform to all related national regulations, standards and recommended specifications as defined by the DICT;
- e. All wireless access points used by staff on the county government's secure wireless network shall follow the DICT standard configuration settings;
- f. Wireless security testing shall be performed on a periodic and random basis using audit penetration tests. However, all penetration tests carried out internally shall have prior approval from the director ICT and the Chief Officer responsible for ICT.

### **3.1.4 Public Internet Access**

To ensure public internet access, the following shall be adhered to;

- a. CGN may provide ICT equipment and software with the correct security provisions either as a publicly available PC or as a hotspot;
- b. Members of staff are responsible for ensuring that equipment is used by the public in accordance with the County Government's ICT Policy;
- c. Members of the public, staff, residents who utilize Guest's wireless access points or specially provisioned networked access points whilst using their own ICT equipment should be made aware of the ICT policy and be aware that any damage to privately owned ICT equipment resulting from incorrect usage is their responsibility;
- d. CGN shall not be held responsible for any financial loss or damage incurred as a result of Internet activity.

### **3.1.5 Cyber and Information Security**

To ensure cyber and information security, the following shall be adhered to;

- a. All individuals and organizations granted access to the CGN's ICT systems shall be responsible for complying with the County's ICT Policy, related guidelines, and procedures;
- b. Users shall take appropriate measures to protect the systems and information they access and shall not copy or share confidential information without authorization from the respective line managers;
- c. Users shall protect confidential information stored or accessed through their accounts, including passwords and login credentials;
- d. Access to County ICT systems shall be allowed only for official County business. Authorized users include county employees, approved contractors, temporary staff, partners, and members of the public using designated public information services;
- e. The County Government shall be committed to fostering a security-conscious culture. All employees shall receive security awareness training relevant to the sensitivity of systems or information they access. Specialized staff will receive role-specific training. Policies and procedures will be readily accessible to ensure users remain informed and compliant;

- f. All County-owned computers and personal devices used for official purposes shall have antivirus software installed, with virus definitions updated regularly. It is the user's responsibility to ensure their devices are kept up to date;
- g. The ICT Directorate shall maintain a high level of network security and shall invest in advanced real-time technologies to detect and respond to threats effectively;
- h. Use of County ICT systems, including email and internet, may be monitored to protect information assets and enforce policy compliance. All suspected or actual security incidents must be reported immediately to the ICT Director or the Chief Officer in charge of ICT. Security incidents will be reviewed and findings will be used to improve security measures and user training under the Corrective and Preventive Action (CAPA) procedure;
- i. The County Government shall develop a Business Continuity Strategy based on risk assessments to ensure the continuity of critical services during disruptions;
- j. Risks to ICT systems shall be managed according to the best practices and standards.

### **3.2 Secure Desk**

To ensure secure desk, the following shall be adhered to;

- a. Physical documents containing confidential information shall be stored in locked desks, cabinets, or secure rooms when not in use;
- b. Portable devices like laptops and PDAs, as well as mass storage devices like USB drives, shall be locked away when not in use;
- c. Computers shall not be left logged on when unattended and should be protected by passwords. When sensitive information is on screen, users should take steps to prevent unauthorized viewing, such as minimizing the window or asking unauthorized persons to move away;
- d. A "locked print" system, requiring a PIN to release documents, shall be the default for all shared devices. Users are responsible for ensuring they collect their documents immediately and for securely disposing of any unneeded personal data.

### **3.3 Encryption and Password Management**

#### **3.3.1 Encryption**

To ensure encryption, the following shall be adhered to;

- a. The encryption standard shall be AES 256 bit, RSA, or a higher standard;
- b. DICT shall establish secure procedures for generating, storing, distributing, and rotating encryption keys;
- c. Encrypt data stored on servers, laptops, and other devices and data transmitted over networks;
- d. Encryption policies and algorithms shall be kept up to date to address evolving security threats and technologies;
- e. Employees shall be trained on the importance of data encryption and the organization's policies;
- f. Robust access controls and user authentication mechanisms shall be implemented to manage who can encrypt and decrypt and access the data;
- g. Regular reviews and audit encryption practices shall be carried out to ensure compliance and effectiveness.

#### **3.3.2 Password Management**

- a. All users shall ensure that their password is not divulged or shared with anyone else;

- b. The county government shall encourage multi-factor authentication to add an extra layer of security;
- c. All users shall not write down and store passwords within the office i.e. in office diaries or paper files;
- d. Passwords shall not be inserted into email messages, SMS messages or other forms of electronic communication with the exception of some systems/processes which may require automatically generated temporary passwords to be sent. These temporary passwords shall be changed as soon as possible;
- e. Passwords shall be stored securely, using password managers or other secure storage methods;
- f. Change passwords at least once every 30 days (with the exception of system level passwords which must be changed quarterly);
- g. Users shall be trained about the policy and best practices for password management;
- h. Password configuration group policy has the following password rules:
  - i. Enforce password history **10** passwords remembered;
  - ii. Minimum password length **8** characters;
  - iii. Account lockout threshold **3** invalid login attempts;
  - iv. Resetting account lockout counter should be after 10 minutes;
  - v. Users are prompted to change password at login **7** days prior to the existing one expiring;
  - vi. All systems should be designed to log off if left idle for a period of more than five minutes.
- i. Passwords shall meet complexity requirements – this forces the use of passwords which shall contain at least four of the following five elements:
  - i. Numeric – (0-9);
  - ii. Uppercase – (A-Z);
  - iii. Lowercase – (a-z);
  - iv. Special Characters (?, !, @, #, %, etc.).

### **3.4 Access Control**

To ensure access control, the following shall be adhered to:

- a. A formal process for tracking visitors, including recording their names, dates, times, and signatures for signing in and out;
- b. All keys for buildings, rooms, and cabinets shall be controlled and logged. This involves a system for signing keys in and out, a record of their serial numbers, and secure storage when not in use;
- c. A CCTV secured perimeter for locations with critical and sensitive information;
- d. Access codes for secure locks shall be changed every 90 days and restricted to authorized personnel. Where possible, biometric access shall be employed;
- e. All staff, including cleaners, shall have proper identification and be aware of security procedures;
- f. Physical layout of offices shall be considered to minimize unauthorized access.

### 3.5 ICT Asset Management

CGN is committed to ensuring that all ICT assets, including hardware, software, and network infrastructure, are systematically identified, recorded, protected, and maintained. Through best practices, robust recording mechanisms, and effective processes, the County ensures accountability, security, and optimal performance of these assets to support cost-efficient and reliable service delivery.

#### 3.5.1 Hardware

CGN recognizes hardware as a critical ICT asset requiring standardized procedures for acquisition, tagging, storage and handling, deployment, usage, tracking, maintenance, replacement and disposal. The following policies shall guide the effective management of all ICT hardware assets:

- a. All hardware shall be procured with the input of the DICT through technical specifications and compatibility guidance;
- b. Desktop computers and laptops shall be accompanied by a valid licence for the operating system, office suite and antivirus specifically purchased for the County Government of Nyeri, approved by the DICT;
- c. Technology dealers shall have a valid certificate from the relevant OEM's;
- d. All acquired hardware shall be tagged with a unique asset label and recorded in the Asset Register managed by the DICT. Updates shall be made promptly upon allocation, transfer, repair, or disposal;
- e. Staff shall ensure secure storage of hardware. Offices shall be locked when unattended, and portable devices (e.g. laptops) stored in lockable spaces. Staff issued with hardware are responsible for its care both within and outside County premises. Removal of equipment for off-site use shall be authorized in writing by the Head of Department and recorded in the Asset Register;
- f. Any movement or reassignment of hardware between staff, departments, or locations shall be spearheaded by the respective chief officer in coordination with the relevant directorate. Such movements shall be logged in the Asset Register, noting new custodianship, location, and purpose. Unauthorized internal transfers or changes shall be prohibited;
- g. Only authorized ICT personnel or approved service providers under the supervision of the DICT may perform hardware repairs or modifications. Unauthorized servicing, upgrades, or tampering is strictly prohibited. All maintenance activities shall be recorded in the Asset Register, including service type, parts replaced, and date;
- h. For planning, budgeting, and replacement purposes, hardware shall be deemed to have reached end-of-life as follows:
  - i. Desktop computers, servers and network equipment: 5 years from date of acquisition
  - ii. Laptops: 3 years from date of acquisition
  - iii. Tablets and mobile phones: 2 years from date of acquisition;
- i. Upon reaching end-of-life, devices shall be evaluated by the DICT to determine suitability for continued use, reassignment, or disposal as per the Public Procurement and Asset Disposal Act;

- j. County officers who are required to access government systems shall be provided with official gadgets;
- k. Employees exiting service shall be required to handover their assigned county ICT assets during clearance.

### **3.5.2 Software**

This policy intervention covers ownership, procurement, licensing, legal compliance, documentation, deployment, installation, handover, software updates and user access of software in CGN. The following policies shall guide on this:

- a. All software developed for CGN ICT assets—whether developed internally or by third parties—shall be considered the property of CGN. These include source code, libraries, documentation, licensing and supporting components required to operate the software.  
Ownership includes all rights to modify, maintain, and deploy the software, regardless of the development arrangement, once handed over and accepted by the County Government;
- b. All software acquisitions shall be with the input of the DICT, regardless of the funding source. The Directorate shall review technical requirements, evaluate compatibility with existing systems, guide on licensing options, recommend standard platforms and tools;
- c. All acquired software shall be properly licensed in accordance with applicable laws and public sector procurement regulations. Pirated, trial or unauthorized software is strictly prohibited;
- d. The DICT shall maintain a centralized ICT software inventory, recording software name and version, purpose and department, number of licenses, licensing type (e.g., single-user, enterprise), source (developed or acquired) and expiry/renewal dates (where applicable). Updates to the inventory shall be made during new installations, upgrades, decommissions, or license renewals;
- e. Only software approved and/or procured with the input of the DICT may be installed on County ICT assets. Installations shall be performed or supervised by authorized ICT personnel, and logged in the software inventory system. Users shall not install personal or unauthorized software and share or duplicate licensed software without approval;
- f. All software developed or acquired on behalf of the County shall be handed over in full, including functional and technical documentation, source code (where applicable), access credentials, licensing certificates or agreements. No project shall be considered complete until a full software handover has been received and reviewed by the DICT;
- g. Version upgrades, and structural changes to software shall follow a formal change control process overseen by the DICT;
- h. Any staff member requiring access to any county software system shall submit a request through their immediate supervisor and approved by the head of the respective unit. Alternatively, the supervisor may initiate the request for account

creation or changes on behalf of the staff member. Accounts shall take the form of firstname.lastname;

- i. Requests for changes to user access rights (e.g., role changes or permission escalations) shall follow the same process. The DICT will process account creation or rights modification only upon receiving requests approved by the supervisor and head of the unit and will maintain an audit trail of all such actions;
- j. During emergencies or data migrations, ICT staff may assist in data transfer. However, system data owners must validate the migrated data within a reasonable period of time.

### 3.5.3 Databases

This policy intervention covers database identification, recording and management. The following policies shall guide on this:

- a. All databases used or managed by County departments—whether hosted internally or externally—shall be listed in an asset register. Including unique identifiers, name, purpose, environment, owner, creation date and status;
- b. All structural or configuration changes to databases—including schema updates, migrations, or platform changes—shall follow a formal change control process coordinated by the DICT.

### 3.6 BYOD

CGN permits the limited use of personal devices for official duties. This policy outlines the responsibilities and processes for managing BYOD:

- a. Only the following user-owned devices are permitted for official County use, subject to approval by the DICT: smartphones, tablets, iPads and Laptops.;
- b. All user-owned ICT devices brought onto County premises for official use shall be registered at the point of entry. The DICT shall maintain a **BYOD register**, capturing user's name and department, device type and MAC address, purpose of use and duration or frequency of access;
- c. Users registered to use personal devices for County work shall ensure proper maintenance and functionality of their devices and prevent physical loss or damage during official use;
- d. The County Government shall not be responsible for repair, replacement, or technical support of personal devices.

### 3.7 Business Continuity and Disaster Recovery

To ensure disaster preparedness and response, the county;

- a. Shall develop a disaster recovery and a business continuity plan;
- b. Shall upgrade the battery energy storage system for the data centers to at least 8 hours capacity;
- c. Shall allocate dedicated funding to support business continuity and disaster recovery initiatives, ensuring that financial limitations do not hinder the implementation of critical resilience measures;
- d. Shall advocate for integrated systems;
- e. May Conduct regular security drills.

### 3.7.1 Incident Categories

Category	Description	Examples
Security	Breach of confidentiality, integrity and availability.	Malware, phishing, unauthorized access etc.
Operational	System or hardware failure	Server crash, network outage etc.
Environmental	External physical threats	Fire, flood, power outage etc.
Human Factors	Human related actions	Accidental deletion, misconfiguration, theft etc.

### 3.7.2 Roles and Responsibilities

Role	Responsibility
ICT Steering Committee	Coordinate detection, containment, and recovery
ICT Strategy Committee	Escalation, resource allocation, and reporting
Office of the County Secretary	Internal and external communication
Office of the County Attorney	Legal and regulatory adherence

### 3.7.3 Incident Response Process

#### a) Detection and Reporting

- i. All staff shall report suspected incidents immediately to their respective chief officer;
- ii. Automated monitoring tools will alert the ICT strategy committee of anomalies.

#### b) Assessment and Classification

- i. Determine severity level and potential impact.

Impact Level	Urgency Level	Priority	Description
Low	Low	Low	Minor issue; monitor and document.
Low	High	Medium	Needs timely attention; potential escalation.
High	Low	Medium	Significant impact; plan response accordingly.
High	High	High	Critical incident; immediate action required.

#### c) Activate the response protocols

- i. Containment;
- ii. Eradication;
- iii. Recovery;
- iv. Post-Incident Review;
- v. Communication;
- vi. Documentation and Reporting;
- vii. Training and Awareness.

### 3.7.4 Data Backup

To ensure the integrity, availability, and recoverability of critical data and systems in the event of a disaster, cyberattack, or system failure, this policy outlines the standards and procedures for backing up digital assets managed by the CGN. Backups will be stored both onsite and offsite, and the Directorate will maintain daily, weekly, monthly, and annual copies.

#### 3.7.4.1 Data Classification for Backup

Classification	Examples	Backup Frequency
Critical Data	Financial Systems	Daily
Important Data	HR Records	Weekly
Archived Data	Historical Records, Old Project files	Quarterly

- a. All backup data shall be encrypted using AES-256 or higher;
- b. Access to backup systems shall be restricted to authorized officers;
- c. Backup logs shall be maintained and reviewed monthly;
- d. Monthly Restore Tests: Simulate disaster scenarios to validate recovery procedures;
- e. Checksum Verification: Ensure data integrity during backup and restore;
- f. Audit Trails: Maintain logs of all backup and restore activities;
- g. Retain backups for a minimum of 7 years or as per legal requirements;
- h. CCTV backups shall be retained for a minimum of one month;
- i. Disposal shall be documented and approved by the ICT Steering Committee;
- j. Annual review of backup procedures;
- k. Feedback loop from disaster recovery drills to refine backup strategy.

### 3.8 Communication

#### 3.8.1 Social Media

The DICT shall have exclusive authority over the activation and deactivation of all official social media platforms operated under CGN.

#### 3.8.2 Email

To enhance the integrity, efficiency, and professionalism of government communication, CGN shall implement the following policy interventions:

- a. Centralized management of the official email system by the Director of ICT;
- b. User accounts shall take the form of firstname.lastname@nyeri.go.ke;
- c. The County Government email users shall be responsible for their own actions;
- d. Chief officers are responsible for enforcing awareness and compliance within their respective departments;
- e. Government issued emails shall be used primarily for official purposes;
- f. The use of personal email services for government communication is prohibited;
- g. Intentional transmission of spam, offensive, defamatory, or copyrighted material is prohibited;
- h. All email users shall comply with the County Government's Data Security, Confidentiality, and Privacy guidelines;

- i. All email communication is subject to monitoring and legal review when policy violations occur;
- j. Implementation of anti-virus and spam filters to detect and contain malware or harmful content;
- k. Users shall maintain professionalism in all email communications;
- l. Email signatures shall include official name, job title, department, organization, county website, physical location and telephone number along with an official disclaimer;
- m. Limits set for email size (maximum 86MB);
- n. Retention and logging practices established for tracking and incident response;
- o. All emails from the County Government shall carry the standard disclaimer below to mitigate legal liability and clarify the nature of the communication.

***“All emails sent from the County Government of Nyeri are subject to its emails terms and conditions”***

#### **3.8.2.1 Email’s Terms and conditions**

- a. Emails and any files transmitted are confidential and may be legally privileged, and are solely intended for the use of the individual or entity to whom they are addressed;
- b. If you receive any email in error, please notify the sender and immediately delete the email from your system;
- c. Any disclosure, copying, distribution or any action taken or omitted in reliance on this, is prohibited and may be unlawful;
- d. The County Government of Nyeri disclaims any liability to the fullest extent permissible by law for any consequences that may arise from the contents of any email sent from its systems, including but not limited to personal opinions, malicious and/or defamatory information and data/codes that may compromise or damage the integrity of the recipient’s information technology systems;
- e. Views or opinions presented in any email are solely those of the author and do not necessarily represent those of the County Government.

#### **3.8.3 County Website**

- a. The official website of CGN is [www.nyeri.go.ke](http://www.nyeri.go.ke), and it serves as the primary online platform for public communication, service delivery, and access to government information;
- b. All content submitted for upload to the CGN’s website shall be accompanied by an official letter signed by the Chief Officer of the originating department and approved by the Chief Officer in charge of ICT. An authorized ICT officer with relevant skills—through the Director of ICT—shall then ensure the content is published on the website, in line with the County’s ICT service charter;
- c. In urgent cases, content may be submitted via official email to [webmaster@nyeri.go.ke](mailto:webmaster@nyeri.go.ke).

#### **3.8.4 Teleconferencing**

- a. Equip official meeting rooms with video conferencing kits (screens, microphones, cameras, UPS power backup, etc.);
- b. Promote teleconference data privacy by controlling who can access recordings;

- c. Regulate recording, storage, and sharing of meeting data; meeting participant only have read only rights;
- d. Require password-protected access, waiting rooms, and controlled admission;
- e. Sharing of meeting links publicly can only be done with official authorization;
- f. Unverified users shall not be allowed to participate in virtual meetings;
- g. Users with aliases such as device name, and non-official names will be denied access;
- h. Only official county emails shall be used to initiate virtual meetings;
- i. The county shall adopt one platform for all its virtual meetings.

### **3.9 Green ICT and Sustainability**

This Policy aims to minimize the environmental impact of ICT use while enhancing energy efficiency, reducing waste, and promoting sustainable development

Through the following measures, ICT will not only support service delivery but also contribute to long-term sustainability and environmental conservation.

The County shall adopt the following measures:

- a. Promote the use of renewable energy sources for ICT infrastructure;
- b. Adopt energy-efficient ICT equipment and implement energy-saving management settings across all devices in the data center;
- c. Promote refurbishment and reuse of ICT equipment;
- d. Require suppliers to meet environmental standards (e.g., energy ratings, recyclability);
- e. Create awareness targeting county staff on Green ICT;
- f. Promoting virtualization of servers and desktops to optimize resource use;
- g. Conduct annual assessment on the environmental performance of ICT systems.

### **3.10 ICT Governance**

ICT governance provides the framework for effective leadership, accountability, and alignment with national priorities. The County will strengthen institutions, modernize infrastructure, expand e-government services, build partnerships, and establish monitoring mechanisms to ensure sustainable ICT development. The County will be guided by the following ICT governance policies to strengthen leadership, ensure accountability, and promote sustainable digital development:

- a. Strengthening Institutional Framework & Leadership by establishing centralized ICT governance units responsible for policy enforcement, strategic planning, and coordination across departments to ensure consistency, accountability, and alignment with the national ICT Master plan and IT governance standard;
- b. The County shall prioritize the expansion and modernization of ICT infrastructure, including broadband connectivity, data centers, and digital access points, with special focus on underserved rural areas;
- c. Nyeri County shall promote e-government platforms to enhance transparency, accountability, and citizen participation in governance, including digital service delivery, feedback mechanisms, and open data initiatives;

- d. The county shall actively pursue strategic partnerships with private sector players, academic institutions, and civil society to foster innovation, resource mobilization, and sustainable ICT development;
- e. The County Government shall establish a comprehensive monitoring and evaluation framework to assess ICT performance, ensure compliance with standards, and inform continuous improvement of ICT initiatives;
- f. All ICT projects shall have a well-defined training, management and implementation plan.

### **3.11 ICT Capacity Development**

To build a skilled, innovative, and future-ready workforce, the County will invest in continuous ICT capacity development. The following interventions will guide efforts to strengthen internal expertise, close skills gaps, and foster partnerships that support professional growth and digital transformation. The ICT steering committee shall:

- a. Conduct ICT skills gap assessment and implement interventions;
- b. Prepare/develop of annual ICT recruitment plan;
- c. Implement comprehensive training programs on emerging technologies, integrate digital skills into staff development, and promote innovation through partnerships, peer learning, and tech-focused initiatives;
- d. Strengthen internal ICT capacity through knowledge transfer, staff mentorship by experts, and retention strategies that support professional growth and recognition;
- e. Build internal capacity through knowledge transfer clauses in consultancy contracts and encourage shadowing and co-implementation models with external experts;
- f. Partner with academia and industry through formal agreements on need basis.

### **3.12 Emerging Technologies**

#### **3.12.1 Cloud Computing**

- a. Adopt a cloud-first/ colocation approach for new ICT systems;
- b. Promote hybrid cloud models for flexibility and business continuity;
- c. Deployed SaaS platform shall be exclusively licensed to the county.

#### **3.12.2 Artificial Intelligence (AI)**

- a. Pilot AI applications in healthcare diagnostics, agricultural forecasting, and citizen feedback analysis.
- b. Build AI literacy among county staff through targeted training.
- c. Establish ethical guidelines for responsible AI use, aligned with Kenya's National AI Strategy 2025.
- d. Collaborate with academic institutions and tech startups to develop localized AI solutions.

#### **3.12.3 Robotics**

- a. Promote robotics for automating repetitive tasks in county operations (e.g., waste sorting).
- b. Support innovation hubs and youth-led startups developing robotic solutions.
- c. Encourage robotics clubs in schools and youth centers.
- d. Monitor global trends to identify viable use cases for local adaptation.

---

### **3.12.4 Blockchain**

- a. Implement blockchain pilot initiatives in areas like licensing, and records management to assess effectiveness before scaling.

---

## **CHAPTER FOUR: MONITORING, EVALUATION, ACCOUNTABILITY, AND CONTINUED LEARNING**

The MEAL system adopted for this policy will be designed to provide feedback to stakeholders to ensure accountability, transparency, facilitate appropriate decisions on future implementation, and review the policy to ensure that the input delivery, work schedules, and target outputs are progressing according to the plan.

This policy shall be evaluated following the overall County monitoring and evaluation framework, standards, and system. The following requirements shall apply regarding policy monitoring and evaluation as set by the department responsible for ICT management:

- a) Designate staff to be responsible for coordinating the monitoring and evaluation of the implementation of this policy;
- b) In each period of 12 months, prepare a report on the progress made in implementing the policy, which shall be submitted to the ICT Steering Committee for consideration and decision-making;
- c) There shall be a policy review every three (3) years or as the need arises which shall involve all ICT management stakeholders, and the report submitted to the County Executive Committee for consideration and decision-making. The review will give input on the execution of the policy's goals and the implementation of the policy;
- d) The policy shall be evaluated at the end of each period of three (3) years to assess the extent to which policy outcomes have been realized including policy impact;
- e) The policy evaluation report shall be disseminated to the relevant stakeholders.

This policy stresses effective MEAL to ensure sustainability, transparency, accountability, and professionalism at all levels. The information will then be linked to the population trends, economic growth, and other social monitoring parameters and thereby provide a basis for policy reviewing and planning of future ICT management needs. The information will also inform on the effectiveness and relevance of the policy.

---

## CHAPTER FIVE: POLICY IMPLEMENTATION

This chapter defines the steps that must be taken to implement the ICT Policy, to include the institutions established for such implementation and the resources required.

### 5.1 Planning and Performance Management

This policy establishes a strong foundational case for ICT as a key pillar in the transformation of County operations, aligning with Kenya's Vision 2030, the Kenya Digital Economy Blueprint, BETA and the County Government's development plans. It articulates the County Government's vision for ICT-led innovation, inclusive access, and improved service delivery, grounded in principles of integrity, transparency, professionalism, security, and citizen participation.

### 5.2 Collaboration

The DICT shall be the liaison for intergovernmental collaboration mechanisms with the national government (MICDE), ICTA and other agencies responsible for matters related to ICT management.

### 5.3 Staff Capacity Development

Having reviewed its staff establishment, the DICT shall, in collaboration with the County Public Service Board and the Directorate of HRM ensure that its staff are equipped with adequate skills and competencies. To enhance existing competencies, the DICT shall register its officers with relevant professional bodies regulating the conduct of ICT professionals. The DICT shall also implement comprehensive training programs and put in place effective knowledge and succession management processes.

### 5.4 Establishment of institutions/committees

To enable implementation of this Policy and per the guidelines of the ICT Authority, the CECM responsible for ICT shall establish and appoint the committees below. The Committees may co-opt such other technical personnel as they may deem fit to enable them better carry out their functions.

#### 5.4.1 ICT Strategy Committee

The Committee shall comprise of all the County Chief Officers and be chaired by the CECM in charge of ICT Management. The Director for ICT shall be the Secretary to the Committee. The functions of the Committee are to:

- a. Decide the overall level of IT spending and how costs will be allocated,
- b. Align and approve the enterprise's IT architecture,
- c. Approve project plans and budgets, setting priorities and milestones,
- d. Acquire and assign appropriate resources,
- e. Ensure that projects continuously meet core objectives of the county government,
- f. Monitor projects, plan for delivery of expected value and desired outcomes, on time and within budget,
- g. Monitor resource and priority conflict between county departments and the ICT functions as well as between projects,
- h. Communicate strategic goals to project teams,
- i. Consider recommendations from the ICT strategy committee.

### 5.4.2 ICT Steering Committee

The Committee shall comprise the Chief Officer for the time being responsible for ICT as the Chairperson and the Director for ICT as the Secretary; other members shall be unit heads within the DICT.

The functions of the Committee are to provide insight and advice to the Steering Committee on:

- a. Make recommendations and requests for changes to strategic plans (Priorities, funding, technology approaches and resources),
- b. The alignment and relevance of the development in and contribution of ICT to the county government's core mandate,
- c. The achievement of strategic ICT objectives,
- d. The availability of suitable ICT resources, skills and infrastructure to meet the strategic objectives of the Directorate and the county government at large,
- e. Optimization of ICT costs, including the role of and value delivery of external ICT sourcing,
- f. Risk, return and competitive aspects of ICT investments,
- g. Exposure to ICT Risks, including compliance risks,
- h. Direction to management relative to ICT strategy.

**ANNEXURE ONE: IMPLEMENTATION MATRIX**

<b>Policy Objective</b>	<b>Policy Strategy</b>	<b>Activities</b>	<b>Actors</b>	<b>Timeline</b>	<b>Status</b>
1. Align with existing national and county legal, regulatory and policy frameworks	Conform to ICTA standards and guidelines for ICT	Establish the ICT Strategy and Steering committees;	CECM in charge of ICT	FY 2025/26	*Steering Committee needs reconstitution *Constitution of the Strategy Committee
		Develop an ICT risk strategy/plan	ICT Steering Committee	FY 2026/27	Pending
		Implement the training policy in line with ICTA standards on human resource development	ICT Steering Committee	FY 2025/26	Pending
		ICT Continuous service improvement through conducting regular system audits	ICT Steering Committee	FY 2027/28	Pending
		Develop standard operating procedures for documenting ICT operations	ICT Steering Committee	FY 2026/27	Pending
		Ensure data security, privacy and business continuity	ICT Steering Committee	Continuous	Requires upgrade
		Accreditation of ICT professionals within the Directorate	ICT Steering Committee	FY 2025/26	Pending
2. Promote innovation and digital inclusion	Facilitate public communication and access to information	Establish and equip ICT hubs across sub counties	<ul style="list-style-type: none"> <li>● CECM in charge of ICT</li> <li>● CECM, Department of Transport, Public Works, Infrastructure and Energy</li> <li>● CECM, Department of Lands, Physical Planning and Urban Development</li> <li>● CECM, Department of Education, Training and Devolution</li> </ul>	FY 2026/27 FY 2027/28 FY 2028/29	Pending

Policy Objective	Policy Strategy	Activities	Actors	Timeline	Status
			<ul style="list-style-type: none"> <li>CECM, Department of Gender, Youth, Sports and Social Services</li> </ul>		
	Facilitate the establishment of structures for citizen participation including information communication technology-based platforms	Train users on e-governance	<ul style="list-style-type: none"> <li>CECM in charge of ICT</li> <li>Office of the County Secretary</li> </ul>	FY2026/27	Pending
3. Adopt emerging technologies and industry trends to enhance efficiency in delivery of the CGN's core mandate.	Capacity Building and Digital Skills Development	Partner with universities, research institutions, and innovation hubs to monitor emerging trends	<ul style="list-style-type: none"> <li>Office of the County Attorney</li> <li>Office of the County Secretary</li> <li>Director, ICT</li> </ul>	FY 2026/27	Pending
		Training of county staff on emerging technologies.	<ul style="list-style-type: none"> <li>CECM, Department of County Public Service and Solid Waste Management</li> <li>Office of the County Secretary</li> </ul>	FY 2026/27	Pending
	Forge Strategic Partnerships and Resource Mobilization	Encourage Public-Private Partnerships (PPPs) for emerging technology projects.	<ul style="list-style-type: none"> <li>Office of the County Secretary</li> <li>Office of the County Attorney</li> <li>ICT Strategy Committee</li> <li>ICT Steering Committee</li> </ul>	FY 2026/27	Pending
		Leverage county's role in the Council of Governors ICT Committee to push for joint innovation programs.	<ul style="list-style-type: none"> <li>Office of the Governor</li> <li>Office of the County Attorney</li> <li>ICT Strategy Committee</li> <li>CECM, Department of Education, Training, and Devolution</li> </ul>	FY 2026/27	Pending
		Tap into national and global funding	<ul style="list-style-type: none"> <li>Office of the Deputy Governor</li> <li>CECM in charge of ICT</li> <li>ICT Steering Committee</li> </ul>	FY 2027/28	Pending

<b>Policy Objective</b>	<b>Policy Strategy</b>	<b>Activities</b>	<b>Actors</b>	<b>Timeline</b>	<b>Status</b>
	Mainstream Emerging Technologies into Service Delivery	Integrate AI-driven analytics for decision-making	<ul style="list-style-type: none"> <li>• ICT Strategy Committee</li> <li>• ICT Steering Committee</li> </ul>	FY 2026/27	Pending
		Adopt e-Government solutions	<ul style="list-style-type: none"> <li>• ICT Steering Committee</li> <li>• ICT Strategy Committee</li> <li>• All County Departments</li> </ul>	FY 2025/26	Continuous
		Deploy GIS platforms for planning, land management, and resource mapping.	<ul style="list-style-type: none"> <li>• All County Departments</li> <li>• ICT Steering Committee</li> </ul>	FY 2025/26	Continuous
		Introduce blockchain for transparent revenue management.	<ul style="list-style-type: none"> <li>• CECM in charge of ICT</li> <li>• ICT Steering Committee</li> </ul>	FY 2028/29	Pending
	Develop Smart County Digital Infrastructure	Establish a modern county data center with cloud and hybrid capabilities.	<ul style="list-style-type: none"> <li>• ICT Strategy Committee</li> <li>• ICT Steering Committee</li> </ul>	FY 2027/28	Pending
		Deploy IoT sensors in sectors like agriculture, health, water, and waste management.	<ul style="list-style-type: none"> <li>• ICT Steering Committee</li> <li>• All County Departments</li> </ul>	FY 2028/29	Pending
		Roll out county-wide broadband and public Wi-Fi hotspots in markets, institutions, and government offices.	<ul style="list-style-type: none"> <li>• Office of the County Secretary</li> <li>• ICT Strategy Committee</li> <li>• ICT Steering Committee</li> <li>• CECM, Department of Trade, Tourism, Culture and Cooperative Development</li> </ul>	FY 2025/26	Continuous
4. Ensure data security, privacy, and continuity of digital services	Strengthen Cybersecurity Infrastructure	Deploy enterprise firewalls, intrusion detection/prevention systems and endpoint protection.	<ul style="list-style-type: none"> <li>• ICT Steering Committee</li> </ul>	FY 2026/27	Pending
		Implement multi-factor authentication (MFA) for all critical systems.	<ul style="list-style-type: none"> <li>• ICT Steering Committee</li> </ul>	FY 2025/26	Pending
		Regularly patch and update systems to close vulnerabilities.	<ul style="list-style-type: none"> <li>• ICT Steering Committee</li> </ul>	FY 2025/26	Continuous

Policy Objective	Policy Strategy	Activities	Actors	Timeline	Status
	Implement Robust Data Protection Measures	Encrypt sensitive data in storage and during transmission.	<ul style="list-style-type: none"> <li>ICT Steering Committee</li> </ul>	FY 2026/27	Continuous
		Enforce role-based access control (RBAC) to limit unauthorized access	<ul style="list-style-type: none"> <li>ICT Steering Committee</li> </ul>	FY 2026/27	Continuous
		Conduct regular data audits to ensure compliance with the Kenya Data Protection Act, 2019.	<ul style="list-style-type: none"> <li>ICT Strategy Committee</li> <li>ICT Steering Committee</li> </ul>	FY 2026/27	Continuous
	Establish Business Continuity and Disaster Recovery (BC/DR)	Develop and maintain a Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).	<ul style="list-style-type: none"> <li>CECM, Department of Gender, Youth, Sports and Social Services</li> <li>ICT Steering Committee</li> </ul>	FY 2026/27	Pending
		Set up data backup systems (on-premise and cloud-based) with automated scheduling.	<ul style="list-style-type: none"> <li>ICT Steering Committee</li> </ul>	FY 2025/26	Continuous
		Perform periodic disaster recovery drills to test readiness.	<ul style="list-style-type: none"> <li>ICT Steering Committee</li> <li>CECM, Department of Gender, Youth, Sports and Social Services</li> </ul>	FY 2025/26	Continuous
5. Enhance stakeholder collaboration;	Implement Centralized Data Sharing and Collaboration Tools	Deploy secure document management and collaboration platforms (e-cabinet, intranet, etc.)	<ul style="list-style-type: none"> <li>All County Departments</li> <li>ICT Steering Committee</li> </ul>	FY 2025/26	Continuous
		Introduce dashboards and reporting tools accessible to all departments.	<ul style="list-style-type: none"> <li>ICT Steering Committee</li> </ul>	FY 2026/27	Pending
	Strengthen ICT Infrastructure for Interoperability	Ensure all systems comply with interoperability standards (APIs, open data standards).	<ul style="list-style-type: none"> <li>ICT Steering Committee</li> </ul>	FY 2026/27	Pending
		Upgrade network connectivity across all sub-counties and offices (SD-WAN, VPNs).	<ul style="list-style-type: none"> <li>ICT Strategy Committee</li> <li>ICT Steering Committee</li> </ul>	FY 2026/27	Pending

<b>Policy Objective</b>	<b>Policy Strategy</b>	<b>Activities</b>	<b>Actors</b>	<b>Timeline</b>	<b>Status</b>
		Provide video conferencing, virtual meeting rooms, and team collaboration software.	<ul style="list-style-type: none"> <li>● ICT Strategy Committee</li> <li>● ICT Steering Committee</li> </ul>	FY 2026/27	Pending
6. Encourage ethical, responsible, and professional use of ICT.	Develop and Enforce ICT Usage Policies and Guidelines	Draft a County ICT code of ethics and acceptable use guidelines.	<ul style="list-style-type: none"> <li>● ICT Steering Committee</li> </ul>	FY 2025/26	Pending
		Enforce compliance through audits, monitoring, and disciplinary measures for misuse.	<ul style="list-style-type: none"> <li>● ICT Strategy Committee</li> <li>● ICT Steering Committee</li> <li>● Directorate of Internal Audit</li> <li>● Office of the County Secretary</li> </ul>	FY 2026/27	Pending
	Build Awareness and Promote Ethical ICT Practices	Conduct sensitization workshops on responsible ICT use, data privacy, and cyber ethics.	<ul style="list-style-type: none"> <li>● ICT Strategy Committee</li> <li>● ICT Steering Committee</li> <li>● Office of the County Secretary</li> </ul>	FY 2026/27	Continuous
		Run county-wide campaigns on digital responsibility for both staff and citizens.	<ul style="list-style-type: none"> <li>● ICT Strategy Committee</li> <li>● ICT Steering Committee</li> <li>● Office of the County Secretary</li> </ul>	FY 2026/27	Pending