# COUNTY GOVERNMENT OF NAKURU

## DEPARTMENT OF EDUCATION, ICT,

## e-GOVERNMENT & PUBLIC COMMUNICATION

# INFORMATION COMMUNICATION TECHNOLOGY (ICT) STANDARD OPERATING PROCEDURES (SOPs)

## TABLE OF CONTENTS

# ACRONYMS

| | |
|---|---|
| CA | Communications Authority of Kenya |
| CIDP | Nakuru County Integrated Development Plan |
| CIP | County ICT SOPs |
| CPSB | County Public Service Board |
| DBA | Database Administrator |
| DPP | Director of Public Prosecutions |
| GIT | Government Information Technology |
| HICT | Head of Information Communication & Technology |
| ICT | Information Communication Technology |
| ICTA | Information and Communications Technology Authority |
| ISP | Internet Service Provider |
| IT | Information Technology |
| MAC | Media Access Control |
| OS | Operating Systems |
| PC | Personal Computer |
| PPDA | Public Procurement and Asset Disposal Act, 2015 |
| SNMP | Simple Network Management Protocol |
| SOPs | Standard Operating Procedures |
| SSH | Secure Shell |
| SUDO | Substitute User Do |
| UPS | Uninterruptible Power Supply |

## OPERATIONAL DEFINITION OF TERMS

Data Centre
Refers to a repository that houses computing facilities like servers, routers, switches and firewalls as well as supporting components like backup equipment, fire suppression facilities and air conditioning.

ICT Equipment
ICT equipment refers to laptops, desktop computers, smartphones, tablets/iPads, power banks, cameras, printers, televisions, projectors, photocopiers and other ICT related accessories.

Network Equipment
Network equipment refers to switches, routers, wireless access points and other networking accessories.

Public Communication
A communication by means of any broadcast, cable, or satellite communication, newspaper, magazine, outdoor advertising facility, mass mailing, or telephone bank to the general public, or any other form of general public advertising.

Consultant
A professional who is engaged by the County Government to provide expert advice in a particular area.

Vendor
A vendor is a person or an entity that sells goods or services to the County Government.

# 1. INTRODUCTION

## 1.1 Background Information

The Department of Education, ICT, e-Government & Public Communication is one of the ten (10) Departments established to deliver services to the citizens of Nakuru County. It is headed by a County Executive Committee Member.

### Vision

The preferred choice for the delivery of innovative and integrated ICT solutions and digital services.

### Mission

To be the best providers of ICT strategies and services, which deliver long term solution based upon our citizens' requirements.

### Mandate

The mandate of the Department is as follows:

a) Promote public digital literacy.

b) Develop and implement County ICT Policies.

c) Enhance access to information.

d) Develop and implement digital connectivity programmes.

e) Facilitate provision of e-Government Services.

f) Structure, provide and promote public communication services for all County departments.

g) Provision of public Wi-Fi in strategic areas like recreational parks, markets, stadia and social halls

h) Promotion of security policies like cyber security and data protection

i) Keeping up and advising on emerging technological changes and trends

j) Provide the structure for acquisition, management and use of Information Technology through the ICT framework.
k) Providing technical and operational support for systems and infrastructure including networks, websites, e-mail systems, databases and applications.

## 1.2 Statement of Purpose

The purpose of this ICT SOPs is to outline the acceptable user guidelines, rules and principles for ICT equipment and services at the County Government of Nakuru. This will guide the County Government on implementing ICT decisions to achieve its objectives. The SOPs  will ensure that there is availability, accountability, less wastage, confidentiality, security and integrity of ICT resources to support all operations in County Departments and service delivery to the public.

The ICT SOPs is fundamental in ensuring applicable checks and balances are in place during acquisition, usage, management, maintenance, storage and disposal of ICT hardware and software systems as well as infrastructure.

## 1.3 Objectives

The SOPs seeks to guide ICT users, system designers and developers on appropriate standards to be adopted. Its specific objectives are as stated below:

a) To ensure proper utilization of ICT resources within the County.
b) To provide guidance in developing a reliable and secure infrastructure conforming to National ICT SOPs 2019, CA, ICTA Standards and compliance to international standards supporting all services in line with the priorities of the County Government.
c) To provide a framework for development and management of ICT network services that will ensure the availability, reliability, enhanced performance and security.
d) To provide a framework, including guidelines, principles and procedures for the development and implementation of Information Systems in the County.

e) To provide guidelines and procedures on the use of Official email address and sharing of content to the County website and social media platforms.

f) To guide Departments carrying out ICT related projects on the procedures to be followed before acquisition, commissioning, implementation, training and support of ICT equipment and systems.

### 1.4 Scope

This SOPs applies to all ICT facilities, equipment, infrastructure and software applications including relevant services such as training, maintenance, consultancies and data protection. It covers any person accessing, developing, implementing and/or using ICT based information and resources owned, managed, supported or operated by or on behalf of, the County Government of Nakuru.

This includes all County staff, partners and members of public accessing services over County ICT resources; persons contracted to develop, repair, or maintain County ICT equipment and suppliers of outsourced services.

### 1.5 Issuance of ICT Equipment

ICT equipment issuance will be based on the nature of office and duties to be performed by staff.

Management of the Department/Entity will be responsible for approving the staff to be issued with ICT equipment depending on their assignments.

## 2. LEGAL FRAMEWORK

The following legal documents and policies form the foundation for the County Government of Nakuru ICT SOPs.

### 2.1 Constitution of Kenya, 2010

### 2.2 County Government Act 2012

### 2.3 The Kenya National Digital Master Plan 2022-2032

### 2.4 National ICT Policy 2019

### 2.5 Data Protection Act 2019

### 2.6 Computer Misuse and Cybercrimes Act No. 5 of 2018

### 2.7 The Public Procurement and Disposal Act 2015 Revised Edition 2016

### 2.8 Nakuru County Integrated Development Plan (CIDP) 2023-2027

## 3.0 INFRASTRUCTURE

a) The department of ICT will collaborate with the National Government, internet service providers and other development partners to ensure fibre connectivity between County headquarters and all departments/entities.

b) To enhance access to public Wi-Fi the department of ICT will collaborate with the National Government, internet service providers and other development partners.

c) All new buildings constructed by or for the County Government must incorporate an appropriate structured cabling system.

## 4.0 HARDWARE

This chapter covers procedures related to acquisition, issuance, movement, storage, surrender and retirement of obsolete ICT equipment.

### 4.1 Acquisition of ICT Equipment

a) All ICT equipment procured by County Departments/Entities must be brand new.

b) Acquisition of ICT equipment must follow and adhere to all laid down procurement procedures.

c) All acquisition of ICT equipment must be done by the ICT Department on behalf of the user departments or entities in compliance with the latest technical and functional specifications.

d) All donor acquired ICT equipment must be deployed in consultation with the ICT department.

e) ICT equipment must be required to conform to the existing security standards as per latest ICTA guidelines.

f) The Department of ICT must develop technical specifications for all ICT systems for purposes of budgeting and procurement. The Department of ICT must also take part in tender evaluation, testing, inspection and acceptance of newly acquired ICT equipment to ensure conformity to the approved technical specifications and standards.

g) All new laptop and desktop computers should be delivered with genuine license for operating system and application software.

h) The Department of ICT in liaison with departments in charge of persons with Disabilities (PWDs) will consult in acquisition of specialised ICT hardware and software.

### 4.2 Inventory Control

a) Departmental HICT must keep an inventory of all ICT equipment within the Department.

b) All acquired ICT equipment must be keyed into the HICT's inventory system with details of the recipient office.

c) The Departmental HICT shall share with the Director ICT their department's inventory list at the end of each quarter.

d) All County Government ICT equipment must be tagged.

### 4.3 Replacement of ICT Equipment

d) ICT equipment must be deemed obsolete after a period of five years from the date of issue.

e) An officer must be eligible for replacement upon surrender of the previously issued equipment.

f) ICT equipment must not be replaced on account of loss or theft unless the issued equipment has been in use for at least three years from the date of issue or with the approval of the Management of the Department/Entity.

g) ICT equipment must not be replaced on account of wear and tear unless the issued equipment has been in use for at least three years.

h) An ICT equipment shall not be liable for replacement unless it is declared unrepairable by the HICT.

### 4.4 Surrender of ICT Equipment

a) Users must surrender any issued ICT equipment before exit of service.

b) Users must surrender the issued ICT equipment to the HICT.

c) The surrender of ICT equipment must be ascertained by the Department of ICT before clearance.

### 4.5 Movement of ICT Equipment

a) ICT equipment movement register must be maintained by HICT.

b) Users must be issued with a gate-pass during movement of any ICT equipment outside the workstation.

c) Any ICT equipment leaving any County office either for repair or being carried away by a third party or contractor must be issued with a gate-pass.

d) Returned ICT equipment must be verified by HICT to ascertain that it is in its intended condition before being accepted.

e) Any user who intends to relocate any ICT related equipment must first obtain authority from the Chief Officer of the Department. Documentation must be filed having the details of the relocation to enable ease of tracking.

f) It is the responsibility of the Officer issued with an ICT equipment to ensure proper care and safety measures are in place during transportation. In case of any damage during transportation, the Officer responsible for the equipment must report to the HICT immediately.

### 4.6 Lost ICT Equipment

a) Users must report any lost ICT equipment to the nearest Police Station and obtain a Police abstract within 24hrs of the occurrence of the incident.

b) Users must thereafter and within 48hrs of reporting to the Police, present the Police abstract and incidence report to the HICT.

c) The HICT will update the inventory register and report to the Departmental Management, Director ICT and development partners where applicable, of the incident.

### 4.7 Retirement and Decommissioning of ICT Equipment

a) The HICT may decommission equipment that is no longer needed in the department. Decommissioning of equipment shall be undertaken through a committee. The decommissioning should be in line with the Procurement and Assets Disposal Act.

b) Equipment may be decommissioned if it becomes redundant or there is a change in IS architecture/technologically obsolete or it has insufficient capacity to handle application and/or user requirements or Where upgradability options have been exhausted or Where equipment has become unsafe. The equipment can also be reassigned to lesser demanding tasks or appropriate environment if it meets the required safety standards

c) The department may dispose of equipment that it deems no longer useful, damaged beyond repair, cannot be upgraded, the repair cost exceeds one–half of the current estimated value, the parts and/or consumables are not available and end of life and no longer supported by the operating environment.

d) Obsolete ICT equipment will be disposed of as stipulated by the Public Procurement and Disposal Act of 2015.

## 5. SOFTWARE

This chapter covers the development, purchase, testing, implementation and maintenance of all software applications developed or purchased by the County Government of Nakuru.

### 5.1 Acquisition of Software

a) The HICT in collaboration with the system users must develop technical specifications for all ICT software applications/systems before acquisition, take part in tender evaluation, inspection, acceptance and maintenance of the system.

b) Software applications/systems must be required `to conform to the existing security standards as per ICTA guidelines.

c) All purchases of software and acquisitions of systems for use in all departments must be done in consultation with the HICT in the department in compliance with the technical and functional specifications.

d) All donor acquired systems/software must be implemented in consultation with the ICT department

e) All ICT software applications acquired by County Departments/Entities must be genuine and up to date.

f) All software and systems together with their documentation acquired for the County whether developed by staff or contracted parties must remain the property of the County. Such software must be used in compliance with applicable licenses, notices, contracts and SLA agreements.

g) Any system that is procured by the County must be hosted at a County Data Centre or County contracted hosting site at the point of acquisition to avoid loss of data in case of breach of contract by the vendor.

### 5.2 Testing, Implementation and Training on Software Applications/ Systems

a) The HICT in collaboration with the system users must test and commission newly acquired software applications/systems.

b) The HICT must offer system support and administration for software applications/systems.

c) The County Government will use standard software environments/platforms for all official laptops, desktops and portable devices. In exceptional circumstances where use of other platforms is necessary, the Chief Officer for ICT and e-Government MUST give approval.

d) The vendor in consultation with the user department, ICT department must provide adequate skills and capacity to system users on usage.

e) Installation of unlicensed and unauthorized software amounts to breach of proprietary rights and it is strictly prohibited.

f) Only HICT/authorized ICT staff are allowed to install software, transfer and update data on official ICT equipment.

### 5.3 System/Software Upgrade and Maintenance

a) The HICT must advise on and conduct regular software/system upgrades to ensure they are up to date and meet emerging user needs.

b) Before any upgrades or maintenance are implemented by HICT or vendors, prior communication must be issued to users not less than 48 hours before the scheduled date.

c) Frequent systems and software audits shall be carried out to eradicate unlicensed and counterfeit software. This is to ensure safety and business continuity.

d) Only HICT/authorized ICT staff/contracted consultants are allowed to conduct system/software upgrade and maintenance.

e) Installation manuals and media must be kept and readily available to the ICT staff that are authorized to support or maintain systems.

f) The ICT Department shall maintain a minimum technical specification for ICT equipment. These specifications will be reviewed twice a year or as the system requirements for new software changes.

g) New systems being installed must have been tested in the test environments and passed all quality checks. A test and quality check log will be maintained indicating the test results.

h) System audit facilities must be enabled on all systems to record all log-in attempts and failures, and to track changes made to systems.

## 6. NETWORKING SOPS

### 6.1 Network Design

a) The County network must be designed and implemented in such a way as to serve all staff at various County offices.

b) All networks must be mapped and documented by the HICT before installation/ implementation.

c) Design and implementation of County networks must be in conformity to the existing standards as per ICTA guidelines.

d) The design and implementation of the County network will take into account emerging technologies and standards where possible.

e) All County networks must be designed to ensure scalability.

f) Network provision for new and refurbished buildings must be made in accordance with the specification published from time-to-time by the County's ICT Department.

g) All new buildings constructed by/for the County Government must incorporate an appropriate structured cabling system.

h) Connections in Sub Counties and other remote sites must consist of the necessary services and related equipment that allow for remote access connectivity to the centralized County network.

i) Design of County networks must incorporate network security protocols.

j) All unused networks (LAN/WAN) must be removed before installation of the new network.

k) Redundant network shall be used where possible to support critical services.

### 6.2 Network Implementation & Maintenance

a) The contracted vendor/consultant/donor must provide the network layout diagram, log in credentials and documentation during handover/after installation to HICT.

b) High levels of availability, reliability and maintenance will be major objectives in the installation and implementation of the County network.

c) The use of monitoring tools, such as network analysers, penetration testing tools or similar software must be restricted to ICT staff who are responsible for network management and security.

d) Installation, configuration, maintenance, and operation of wireless networks serving on any property owned or rented by the County Government, will remain the responsibility of HICTs.

e) Installation of independent wireless communication equipment is prohibited. Request for installation of wireless device must be approved by the Chief Officer of the relevant Department and must be effected by the HICT.

## 7. INTERNET USAGE

This procedure shall apply to all users who will have internet access through the County's ICT infrastructure. This includes internet and public Wi-Fi provided by the County government.

### 7.1 Resource Usage

a) The County Internet service must be used for official purpose.

b) Websites with heavy load and high traffic will be restricted during peak official hours by use of firewalls. Firewalls will be used to protect the County Government of Nakuru network from unauthorized access or external threats emanating from other networks and regulate use of internet service.

c) Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of internet "wallets" do so at their own risk.

## 8. MAINTENANCE SOPS

Maintenance includes, but is not limited to software changes, hardware changes, network changes, patches, fixes or cabling.

### 8.1 Maintenance and Troubleshooting of ICT Equipment

a) Maintenance of ICT equipment must either be outsourced or done internally by authorized ICT staff. This must be in accordance with existing warranty and maintenance agreements with vendors.

b) For any hardware problem, the user must inform the HICT in the Department at all times for assistance.

c) Only authorized technical personnel from the ICT Department/vendor/donor/partner shall be allowed to modify, repair or reconfigure any ICT related equipment.

d) Authorized ICT personnel must have full access to County owned ICT equipment for purposes of conducting maintenance function.

e) Individual users must not install software or physical devices that prevent authorized ICT staff from accessing the equipment or software to conduct management or maintenance functions.

f) ICT equipment that is powered directly from the main power outlet must be installed with clean power to protect against damage in the event of power fluctuations. Users are required to promptly report faulty UPS devices to the HICT for replacement.

g) Any ICT equipment that is not in use must be powered off as a preventive maintenance measure.

h) Preventive Maintenance of ICT equipment must be done on quarterly basis or when need arises.

i) The HICT must maintain a maintenance log of all repairs/maintenance done within their department.

j) Written notice of all scheduled maintenance must be provided to users, stating the nature of the change, system impact as well as documenting the starting time and duration of the maintenance.

k) HICT shall undertake regular surveys to identify obsolete equipment for the purposes of disposal. Where such equipment contains data, that data shall be backed up and then erased from the device using suitable mechanisms (e.g. equipment sanitization) in line with Government Information security standards.

l) HICT unit shall periodically conduct assessment/audit of ICT equipment to ensure compliance with performance standards and requirements, and ensure equipment component parts are as indicated in the inventory.

### 8.2 Software Maintenance

a) System software will be regularly maintained to ensure they meet the changing requirements of the various users and changes in technology.

b) For systems maintained by contractors, a Service Level Agreement has to be maintained and any maintenance will be carried as per the Service Level Agreement.

## 9. EMAIL & WEBSITES

The ICT Department shall be responsible for the management of official email accounts and County website with authority from the Chief Officers of the user department.

### 9.1 SOPs on Usage of Emails

a) The ICT Department must provide the County Government staff with official email addresses. All official communication MUST be done using the official email addresses.

b) The use of unofficial email address such as Yahoo, Gmail, fast mail…etc. for official communication is unacceptable.

c) Format for official email addressing shall be; FirstName.Surname, domain name being @nakuru.go.ke. e.g. john.smith@nakuru.go.ke Format for Departmental email address shall be; Department Name @ domain name e.g. ict@nakuru.go.ke.

d) All use of email must be consistent with County Government of Nakuru policies and procedures of ethical conduct, safety and compliance with applicable laws and proper business practices.

e) In the event of staff exit from service, the official email account must be de-activated immediately. In the event of staff reinstatement to service, the email account must be re-activated.

*f)* A disclaimer will be generated at the footnote of each email sent that reads: *"This email (including any attachments) is confidential and intended only for the use of the addressee. It may contain information covered by legal, professional or other privilege, which privilege is not lost or waived by mistaken transmission thereof. Unless you are the intended recipient, you may not read, print, retain, use, copy, distribute or disclose to anyone the message (including any attachment) or any information contained in the message. Internet communications are not safe or secure hence the County Government of Nakuru does not accept any legal responsibility for the contents of this message. If you are not the addressee, please inform the sender immediately and destroy this email (including any attachment)."*

g) Sensitive confidential material must NOT be sent through electronic mail unless it is encrypted.

### 9.2 SOPs on Website

a) The ICT Department must undertake appropriate measures that will ensure access to information and knowledge for all through the County website.

b) The Web Administrator shall maintain the County web server and login credentials to upload publications to the main County Government web server (www.nakuru.go.ke).

c) The Web Administrator must identify, evaluate, and provide technical support for software tools for the creation of official Web pages.

d) The County ICT Department must ensure that downtime of the official County website is minimized.

e) The web administrator must consult with authors on the appropriate tools for their needs and provide instructions concerning creation and maintenance of official County Web pages.

f) Department content shall be developed by communication officers and forwarded to the web administrator for uploading to their departmental web pages.

g) The Chief Officers for the various departments must give approval before any information regarding their departments are uploaded online.

h) The County Government website must utilize the County Government logo and branding with corporate colours.

i) Hosting of Departmental websites/pages, must be an extension of the County's main web domain.

j) Departments that have independent web pages must ensure that they are linked to the County Government's main Home page except gazetted city and municipal boards.

k) The department of ICT in consultation with the department in charge of PWDS will put in place features that will make the County website PWD compliant.

### 9.3 Social Media Use

This SOPs provides guidance for employee use of social media platforms and other sites and services that permit users to share information with others in a contemporaneous manner.

a) Only the County Government authorized Communication Officer(s) is/are permitted to post material on social media platforms in the County's name and on its behalf. Any breach of this restriction will be subjected to disciplinary process as guided by code of conduct and any other applicable law.

b) County staff must be sensitized on the effect their social media content may have on their reputation, as well as the County Government's reputation.

c) Employees must not publish, post or release any information that is considered confidential or not meant for public consumption.

d) Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Staff should hence refer these enquiries to the authorized County Government director Public Communication.

e) If any staff encounters a situation while using social media that threaten to become antagonistic, he/she should disengage from the dialogue in a polite manner and escalate the matter to relevant Authorities.

## 10. MEDIA ENGAGEMENT

Only authorised staff are allowed to respond to official matters in the media. This will go a long way in cubbing miscommunication, falsification and protecting the County Government and officers from bad publicity while safeguarding its integrity.

Authorised officers selected to represent the County Government MUST seek prior authority from their immediate supervisor or heads. In line with this, any interviews with media, bloggers or live station interviews MUST be communicated to the immediate supervisor for advice, preparation and equipping. Any interviews with media, bloggers or live station interviews that have not been communicated to heads of departments or immediate supervisor shall be taken as personal opinions and the officer held responsible for the same.

## 11. SECURITY

### 11.1 Ownership

a) While the ICT Department is committed to the provision of a reasonable level of privacy, it shall not guarantee confidentiality of personal information stored or transmitted on any network or device belonging to the County Government. The data created and transmitted by users on the ICT systems must always be treated as the property of the County Government.

b) The ICT Department must protect the County Government's networks, data and systems. It shall not guarantee protection of personal data residing on County's ICT infrastructure.

c) The ICT Department must reserve the right to audit networks and systems on a periodic basis to ensure compliance with this ICT SOPs.

### 11.2 Data Security

a) All County Government work must be done on secure networks preferably within the office network.

b) In case an employee is out of the office and decides to carry part of work with him/her, it will be his or her sole responsibility to ensure that the data contained therein remains confidential. Working in areas such as cyber cafes or other public networks is strictly prohibited.

c) County employees must ensure integrity and confidentiality of County information to avoid breach of data.

d) County employees must ensure that privacy is maintained on their ICT equipment to avoid leakage of privileged information/data. Incase a breach or leakage is detected, the employee must report the case immediately to his/her Supervisor.

e) County Government's data contained in ICT systems must be classified as either confidential or non-confidential. Employees must take all necessary steps to prevent unauthorised access to confidential information like hard disk encryption.

f) In the event of a hardware malfunction and the device needs to be repaired by a third-party, the device hard drive should be backed up to a secure storage device and wiped securely prior to being handed over to an external technician.

### 11.3 General Computer Security

a) All office Computers must run standard supported antivirus software, and must be configured to perform regular updates.

b) Once discovered, any virus-infected computer must be removed from the County network until it is verified as virus-free to avoid spreading of the virus.

c) Users will report security problems with internet use, breach of confidentiality, and any violations of this or other policies and procedures occurring during internet use.

d) End user equipment data protection shall be in line with the government Information Security standards.

### 11.4 Physical Computer Security

a) Portable equipment such as LCD projectors, switches and routers must be stored in secure lockable cabinets.

b) All external windows to rooms containing computer equipment visible to the public must be fitted with window blinds to obscure filming.

c) All entry points giving access to the room or area with computer equipment both from within and outside the building, must be, as a minimum, be fitted with supplementary metal grills.

d) Rooms and buildings incorporating high-density computer equipment such as server rooms, digital hubs must have an access control mechanism installed.

e) Detection devices, such as CCTV cameras, must be installed at strategic locations to ensure that unauthorized access is not possible without detection.
f) Desktops shall be fitted with padlocks to prevent theft of internal devices in the CPU.

### 11.5 Server Security

a) Computer servers must be housed in a room with adequate air conditioning system in order to provide a stable operating environment and to reduce the risk of system crashes due to component failure.
b) Where possible the floor within the server room must be a raised false floor to allow computer cables to run beneath the floor reducing the risk of damage to computer equipment in the case of flooding.
c) Power feeds to the servers must be connected through uninterrupted power supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure.
d) The data centre and server room(s) must have dedicated alternate power backup i.e. generator or solar power to protect the computer systems in case of power failure.
e) Access to the data centre and server room(s) must be restricted to authorized staff only. All non-ICT staff/vendors working within the data centre/server room must be supervised.
f) User access right s and privileges on a server must be controlled based on the role a user requires to perform the desired function(s).

### 11.6 Data centre

The data centre shall adhere to the following guidelines:

a) Security Protocols:
    - Access Control: Define who has access to the data centre, including physical and digital access.

- Authentication Measures: Implement multi-factor authentication for personnel accessing critical systems.
- Surveillance: Install CCTV cameras for monitoring physical access.
- Encryption: Data at rest and data in transit should be encrypted to prevent unauthorized access.
- Intrusion Detection Systems (IDS): Deploy IDS to detect and respond to any unauthorized activities.
- Security Updates: Regularly update software and firmware to patch vulnerabilities.

b) Physical Infrastructure:

- Location: Choose a secure location away from potential hazards like flood-prone areas or earthquake zones.
- Environmental Controls: Implement measures to regulate temperature, humidity, and airflow to ensure optimal equipment performance.
- Fire Suppression: Install fire detection and suppression systems to mitigate the risk of fire damage.
- Redundancy: Have redundant power sources, cooling systems, and network connectivity for uninterrupted operation.
- Equipment Placement: Properly organize racks and equipment to maximize space and airflow.

c) Data Handling Policies:

- Data Classification: Classify data based on sensitivity and implement appropriate access controls.
- Data Retention: Define policies for data retention and disposal to comply with legal and regulatory requirements.
- Backup and Disaster Recovery: Establish regular backup procedures and a disaster recovery plan to minimize data loss in case of emergencies.

d) Compliance and Regulations:

- Regulatory Compliance: Ensure compliance with relevant regulations and industry standards for information security management such as ICTA Data centre Standard ICTA.2.002:2019, ISO 27001, ANSI/TIA-569-c, ANSI/TIA-568-c, ISO/IEC 60793, IEEE, 802.3 and many others
- Follow Auditing and Reporting: Conduct regular audits to assess compliance and generate reports for stakeholders.

e) Resource Management:

- Capacity Planning: Monitor resource utilization and plan for future growth to avoid bottlenecks.
- Energy Efficiency: Implement energy-efficient technologies to reduce operational costs and environmental impact.
- Asset Management: Maintain an inventory of hardware and software assets to track usage and ensure proper maintenance.

f) Personnel Training and Awareness:

- Training Programs: Provide regular training sessions for data centre staff on security protocols, emergency procedures, and compliance requirements.
- Awareness Campaigns: Raise awareness among employees about their roles and responsibilities in maintaining data security.

g) Vendor Management:

- Vendor Selection: Choose reputable vendors for hardware, software, and services, considering factors like security, reliability, and support.
- Contractual Agreements: Clearly define service level agreements (SLAs) and security requirements in contracts with vendors.

h) Emergency Response Plan:

- Incident Response: Develop procedures for responding to security incidents, including containment, investigation, and recovery.
- Communication Plan: Establish a communication plan to notify stakeholders, authorities, and affected parties in case of emergencies.

i) Documentation:
   - Document all policies, procedures, configurations, and changes for future reference and auditing purposes.
   - Regularly review and update documentation to reflect changes in technology, regulations, or business requirements.

j) Continuous Improvement:
   - Conduct regular assessments and reviews to identify areas for improvement and implement necessary changes.
   - Stay updated on emerging technologies, threats, and best practices in data centre management.

### 11.7 Network Security

a) All network cabinets must be kept locked at all times and access restricted to authorized ICT staff only.

b) All networks must be secured through installation of security solutions such as firewalls.

c) Access to the county networks by unauthorized users is strictly prohibited.

d) Users are prohibited from sharing login credentials with unauthorized users.

### 11.8 Password Security SOPs

a) All users are responsible for safeguarding their system access login and password credentials and must comply with the password parameters and standards identified in this SOPs.

b) Passwords must be changed immediately upon issuance for the first-use. Initial passwords must be securely transmitted to the individual.

c) Passwords must never be shared with another individual for any reason or in any manner not consistent with this SOPs. A shared or compromised password is a reportable security incident.

d) Passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats on untagged (unsupported) devices.
e) Users must log out from applications or systems after use (CTRL+ALT+DEL).
f) Passwords should not be shared with an external technician.
g) Passwords must be changed at the regularly scheduled time interval or upon suspicion or confirmation of a compromise.
h) Privileged users consist of users with high level administrative rights. These accounts must have their passwords changed every ninety (90) days.
i) In the event a breach or compromise is suspected, the incident must be reported to the HICT immediately.

### 11.8.1 Password Requirements

The following parameters indicate the minimum requirements for passwords for all user accounts, as indicated below:

a) Contain both upper and lower case characters.
b) Have digits and punctuation characters as well as letters such as 0-9, !@#$
c) Be at least eight characters long.
d) Are not based on personal information, or names of family, among others.

### 11.8.2 Systems Processing Passwords

All County Government systems including servers, applications, and websites that are hosted by or for the County Government must be designed to accept passwords and transmit them with proper safeguards.

a) Passwords must be prohibited from being displayed when entered.
b) Passwords must never be stored in clear, readable format (encryption must always be used).
c) Passwords must never be stored as part of a login script, program, or automated process.

d) Systems storing or providing access to confidential data or remote access to the internal network must be secured with multifactor authentication.
e) Password hashes (irreversible encoded values) must never be accessible to unauthorized individuals.

## 12. BACKUP SOPS

### 12.1 System Backup

a) Backup copies of essential data and software must be taken regularly to ensure that all essential data and software can be recovered following a computer disaster or media failure.
b) Backup copies must be regularly checked to ensure that they can be relied upon when need arises.
c) Backup information, together with accurate and complete records of the backup copies, must be stored in a remote location.
d) Additional backups must always be taken after structural change to the database and/or operating system's file system so as to ensure successful restores in the event that database or system crash (failure) occurs after the structural change and before scheduled backup.
e) The department must ensure that system vendors must leave a database with a backup that can be restored for ease of access to previous records.
f) After the end of the contract, the vendor/partner/donor must not use the County's back up data unless authorised by the County Government.
g) HICT must maintain a Back-up Inventory file which shall document all backups carried out on the critical systems. This shall provide mechanisms for quick monitoring and tracking of scheduled back-ups.

## 13. ICT CAPACITY BUILDING AND TRAINING

### 13.1 Capacity Building and Training of Staff

a) ICT staff employed must have ICT qualifications

b) New staff must be inducted on ICT SOPs, usage and responsibilities.

c) The ICT Department must provide adequate basic and operational training to impart knowledge and skills to new staff members upon entry to service.

d) Staff training on basic ICT skills must be conducted periodically by the ICT Department in liaison with the relevant Departments with an aim of boosting the staff capacity.

e) Training must be carried out in such a manner that all ICT staff undergo continual capacity training so as to be up to date with market trends and technology.

f) The ICT Department must conduct training needs assessment for its staff at the beginning of the financial year and forward the same to the Departmental HR committee for approval.

g) The ICT Department in conjunction with line Departments must facilitate specialized ICT training to staff members upon request.

h) All system users must be trained on acquired systems.

### 13.2 Digital Hubs/Centre

a) The ICT Department shall oversee the operations, maintenance, and strategic direction of all county digital hubs. This includes managing the hardware, infrastructure, software, data and physical security at the digital centre.

b) The ICT Department and/or in partnership with other Departments, partners and stakeholders will conduct training to citizens at Digital hubs.

c) The ICT Department and/or in partnership with line Departments, partners and stakeholders can organize seminars/workshops for innovators to showcase their talents at digital hubs.

d) The County shall engage partners in conducting programmes at the digital hubs through collaboration, funding and building relationships to achieve mutual success.

e) The ICT department in collaboration with the County Inspectorate Unit and National security organs shall ensure security at the digital hubs.

f) The County shall formally engage partners who seek to support the running of programmes through signed contracts and MOUs.

g) The ICT Department will develop a standard programme for conducting training at digital hubs.

h) Digital hubs shall be housed in County owned infrastructure. Where Digital hubs are housed in infrastructure which are not County owned, the County Government shall sign an MOU with the infrastructure provider.

i) Digital hubs are accessible to members of the public. When there is no formal training or programme going on at the Centre, members of the public are free to use the facility as an incubation hub, to do research, access Government services and any other form of ICT innovation. This will be guided by the standard operating procedures of the digital centres.

j) The Department of ICT through sensitization forums and other County Government platforms will create awareness on County Digital hubs and its programmes.

k) The County Government will be responsible for staffing and operating expenses at the Digital hubs.

l) The County shall control access to public Wi-Fi at the digital hubs to avoid misuse and access to explicit content as per the SOP.

m) All activities conducted at the Digital hubs shall be approved by the Chief Officer in charge of ICT.

n) Department of ICT in consultation with relevant departments, will ensure the digital hubs are equipped with specialised hardware and software equipment for people with disability (PWD).

## 14. DATABASE ACCESS AND USAGE

All County Government of Nakuru employees and service providers must adhere to the following policies, processes, and standards related to database management.

### 14.1 Database Ownership, Administration and Management

a) Where the County Government has outsourced services of an external service provider, all the databases handled by such provider must remain property of the County Government.

b) Where the County Government has developed in-house, purchased and/or received a donated system, all the databases and their credentials such as passwords must be shared using proper safeguards with the ICT Department.

c) The application software back up database must be accessible after the termination of the contract with the vendor/donor/consultant.

d) The database administrator must be HICT.

e) Databases holding critical County data must be hosted at a County owned data centre, Government owned data centre or County contracted hosting site to avoid loss of data.

f) The County must have full ownership of databases holding critical County data.

g) All personnel assigned to develop databases and any other software for the county government will be required to create and avail both user and system documentations i.e. Software Design, Source Code Documents, Testing Requirements and end-User Instructions to the Chief Officer Department of ICT. This will ensure ease of maintenance of the databases when need arises.

h) Every database update and maintenance processes must be communicated prior and clearly documented. Replicate at system SOPs

### 14.2 Database Access Privileges

a) All administration processes that require managerial level authorization and supporting utilities for database users must be defined by the Chief Officer of the User Department and Chief Officer Department of ICT.

b) Authorization into databases by applications must be approved by the Chief Officer of the relevant department and will be managed by the DBA.

c) Each database must have security procedures for authorization for access, input and verification, maintenance, periodic review and monitoring of user access.

d) Every user of the database and its components must be assigned access right(s) to determine the extent to which such a user will operate the database.

e) Database usernames and passwords should be stored in a file separate from the executing body of the program's code. This file must be encrypted.

## 15. BRING YOUR OWN DEVICE (BYOD)

a) Employees are prohibited from hosting County owned systems on their personal devices. County systems should be hosted on official devices.

b) Employees allowed to use their personal IT equipment for work purposes must ensure they are secured against malicious software (such as malware) to safeguard County data.

c) The following classes or types of data are not suitable for BYOD and are not permitted on Personally owned Devices:

   i. Anything classified as SECRET or CONFIDENTIAL;

ii. Other currently unclassified but highly valuable or sensitive information which is likely to be classified as SECRET or CONFIDENTIAL.

d) Device users must ensure that valuable data created or modified on the devices are backed up regularly on official County storage.

## 16. GENERAL GUIDELINES

a) The Administrators of ALL systems must be from the ICT Department and appointments will be done by the Chief Officer ICT Department in conjunction with the Chief Officer of the User Department.

b) During the budgeting cycle, the HICT must give proposals, specifications and budget estimates for the planned ICT projects in the Department.

c) ICT equipment and facilities can be used for revenue generation with the approval of the Chief Officer responsible for ICT. This should not affect the effective running of normal programmes of the Department, Entity or Unit.

d) Critical County data shall be safeguarded in accordance with the provisions of the Data Protection Act 2019

## 17. MONITORING, EVALUATION AND REVIEW

### 17.1 Monitoring and Evaluation (M & E)

Realization of the output of this SOPs must require consistent monitoring and evaluation of the output indicators. The County Government and any other relevant stakeholders will carry out monitoring and evaluation. A monitoring and evaluation framework must be developed to ensure midterm review of the SOPs.

### 17.2 SOPs Review

a) This SOPs shall be reviewed every five (5) years in order to be in line with the technological changes in ICT.

b) During review, the Draft SOPs must be subjected to stakeholder participation before it is forwarded for approval by the County Executive.

c) During review, the SOPs must take into account emerging technologies and trends.

## 18. SOPS IMPLEMENTATION & COMPLIANCE

### 18.1 SOPs Implementation

a) The SOPs must be submitted to the County Executive for approval.

b) Once approved, the department of ICT shall publish and publicize the SOPs.

c) The department of ICT shall sensitize all staff on provisions of the SOPs.

d) During acquisition of ICT equipment, Accounting Officers must adhere to the provisions of this SOPs. HICTs will advise on technical specifications for the various tiers of users.

e) The department of ICT shall provide mechanisms for collection of feedback from users.

### 18.2 Compliance

a) This SOPs applies to all staff of County Government of Nakuru and any institution that will share its ICT infrastructure or has access to the County Government's ICT facilities.

b) It is the duty of HICT in the Departments to ensure that staff within their stations are aware of their responsibilities under this SOPs.

c) Staff members currently in service and those joining the County Government shall be required to sign the ICT SOPs acknowledgement and compliance form stating that they have read and understood the contents therein.

d) Violation of this SOPs by any party may result in action being taken against an individual in accordance to the County Government of Nakuru disciplinary and legal mechanisms.

## REFERENCES

i. Constitution of Kenya, 2010.

ii. County Government Act, 2012

iii. Executive Order No. 1 of 2023.

iv. Government of Kenya Cyber Crime Act, 2015

v. Kenya Power Information Technology & Telecommunications SOPs.

vi. National ICT SOPs, 2019.

vii. Public Procurement and Disposal Act, 2015

viii. The Data Protection Act, 2019.

ix. The Kenya National Digital Master Plan 2022-2032