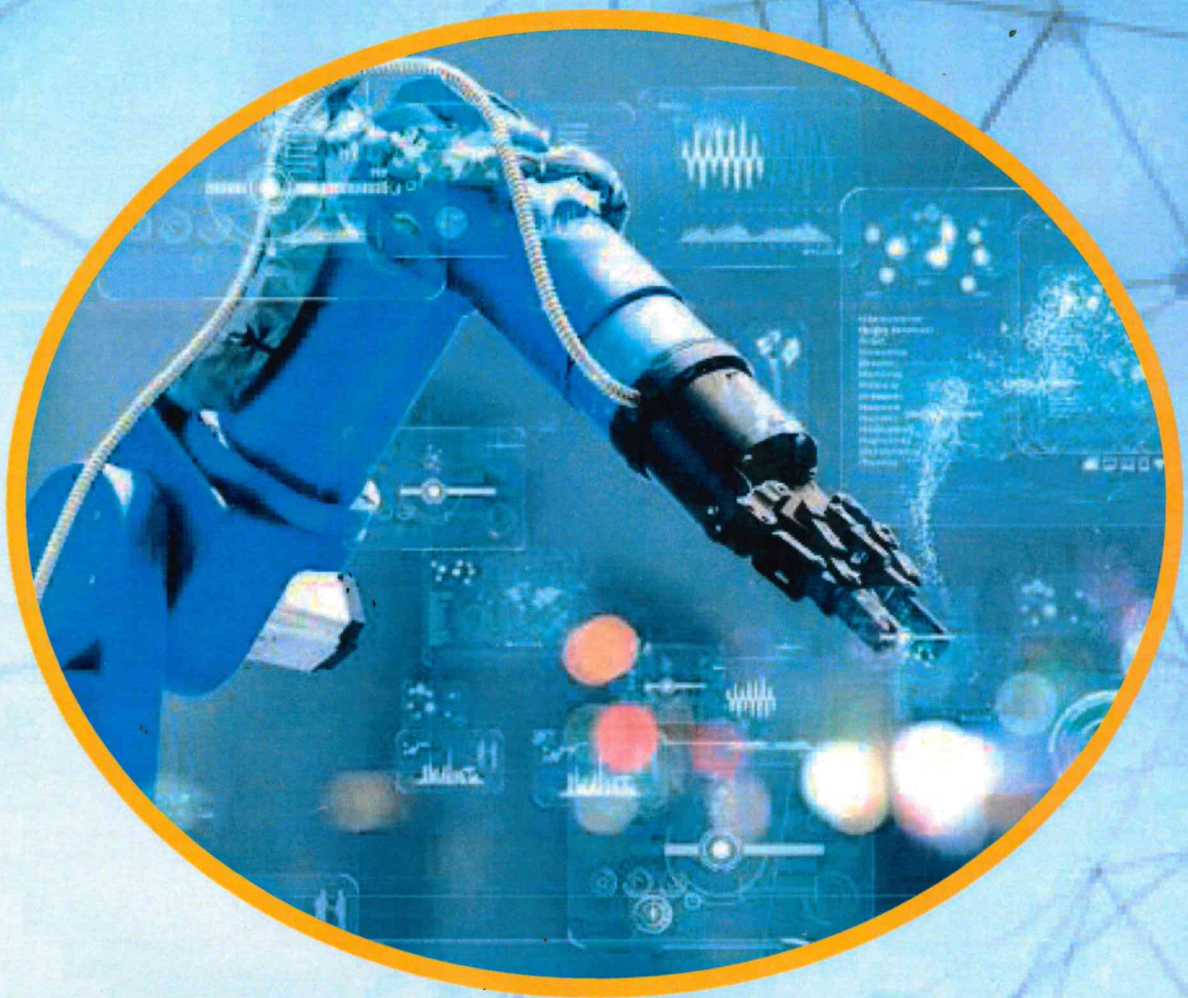
County Assembly of Kisumu



ICT POLICY

September, 2022

COUNTY ASSEMBLY OF KISUMU

INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

SEPTEMBER, 2022

TABLE OF CONTENTS

FOREWORD

This policy is developed against the backdrop and realization of the importance of entrenching ICT in our institutional operations for purposes of ensuring efficiency and effectiveness. The objective of this Information Communication Technology (ICT) Policy is to guide the mainstreaming of ICT in the operation of the County Assembly of Kisumu. We are aware that a functional ICT system improves operational efficiency and overall turnaround time in all service points. The growing importance of ICT in supporting operations of the Assembly cannot be gainsaid.

The concept of ICT starts with policies relevant to information systems that support all service areas, which form the basis for fulfilling the mandate of legislation, oversight and representations. This policy provides guidelines on integrating the information systems within the Assembly for improved service delivery.

Information Technology is essential in ensuring that information systems operate as expected with the human resource acting as a catalytic ingredient that will determine how systems will perform to assist the Assembly in discharging its mandate. The users further develop, operate and manage information systems and information technology resources. Without a proper guiding tool, the users may either misuse, fail to appropriately use or even risk destroying the ICT systems within the Assembly. This policy seeks to fill this gap by offering appropriate user guidelines in order to comprehensively and appropriately streamline the utilization of the ICT systems.

This policy goes beyond these elements in two important ways. First, it seeks to ensure that these essential elements are safeguarded and, secondly, that there is a

recovery strategy in the event of failure. It is for this reason that the ICT Policy contains strong elements on security and business continuity policy statements.

The County Assembly of Kisumu hopes that all users shall bear the responsibility of ensuring that the policy is effectively utilized even as the management plays its role by ensuring that all the relevant stakeholders and users are adequately sensitized on this policy. Upon approval, this policy shall be readily available for access through our website www.kisumuassembly.go.ke .

MR. OWEN OJUOK

COUNTY ASSEMBLY CLERK

ACRONYMS

BIA	Business Impact Assessment
BCM	Business Continuity Management
BCP	Business Continuity Plan
CAK	County Assembly of Kisumu
HR	Human Resource
ICT	Information Communication Technology
ID	Identity
PC	Personal Computer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
CASB	County Assembly Service Board

DEFINITION OF TERMS

Administrators:	Person responsible for management of a particular aspect of ICT resources
Alternate Site:	Alternate Site means a site held in readiness for use in the event of a major disruption that maintains an organizations' business continuity.
Business Continuity:	A state of continued, uninterrupted operation of a business.
Chain email:	An email that in the body or subject of the message requires the recipient to forward the e-mail on to multiple people.
Crisis:	It is an event, occurrence and/or perception that threaten the operations of members, staff, brand, reputation, trust and/or strategic/business goals of the Assembly.
Disaster:	This is a sudden, unplanned catastrophic event that compromises the assembly's ability to provide critical functions, processes, or services for some unacceptable period of time, causing unacceptable damage or loss.

Emergency Response Team: It's any organization or department that is responsible for responding to hazards to the general population (e.g. fire brigades, police services, hospitals, ICT department)

ICT (Information Communication Technology): ICT means technologies, including computers, telecommunication and audiovisual systems, that enable the collection, processing, transportation and delivery of information and communications services to users.

ICT System: An ICT system definition includes, but is not limited to, hardware, software and communications equipment that the Assembly uses to communicate, process and store information. The organization and structures involved in relating all these systems, the information they store and the people involved in the administration and maintenance within the Assembly or outside the Assembly.

Individual Access Controls: Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner.

Insecure Internet Links: Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of CAK.

Security Breach: Accessing data of which an employee is not an intended

recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Operational Risk: It means the risk of loss from inadequate or failed internal processes, people and systems or from external events.

Portal: An organization's data/information resource accessed via internet for public usage

Recovery: This is the rebuilding of a specific business operation following a disruption to a level sufficient to meet outstanding business obligations.

Sensitive information: Data that must be protected from unauthorized access to safeguard the privacy or security of staff, members or the Assembly.

Unauthorized Disclosure: The intentional or unintentional revealing of restricted Information to people, both inside and outside CAK, who do not have a need to know.

User: A user means any person who is recognized by the Assembly as having a valid reason to access the Assembly ICT systems whether that access is from

within or outside the Assembly

STATEMENTS OF IDENTITY

Vision: To be a model, independent and people responsive County Assembly in Kenya

Mission: To provide a premier legislation, oversight and representation services that promotes the socio-economic development to the residents of Kisumu.

Core Values

Integrity: We allow positive criticism and empower staff to promote accountability, transparency and acceptable work ethics prescribed in code of conduct and as per Chapter Six of the Constitution.

Professionalism: We advocate for honest meritocracy at all levels from recruitment to consistency in efficient service delivery

Respect: We exercise due regard to the feelings, wishes and rights of staff, MCAs and citizens at all times

Inclusivity: We encompass everyone including special interest groups by focusing on our people and stakeholders through win-win arrangements to support devolution and democratic.

Communication: We promote effective exchange of clear information within the Assembly and outside by listening, understanding and receiving feedback on addressing critical issues.

Teamwork: We are having good working relationship as CAK team and while at the same time recognizing individual performers in the teams

Equity: We treat our staff, MCAs and citizens in a fair and impartial manner, regarding distribution of information, resources, and participation.

1.0. INTRODUCTION

1.1 Background

In discharging her roles of legislation, oversight and representation, the County Assembly of Kisumu, herein after referred to as CAK, acquires, installs and uses ICT hardware and software in enhancing efficiency and effectiveness of its services. This policy intends to govern the effective utilization of the ICT infrastructure within the County Assembly of Kisumu.

The ICT (Information Communication Technology) refers to technology that is used for processing and distribution of data/information using computer Hardware and Software, Telecommunication and Digital electronics. The use of ICT enhances efficiency, and effectiveness in discharging the legislative, oversight and representation roles of the County Assembly.

The County Assembly of Kisumu is a live to the fast changing and advances of the world that has poised the concept of globalization through enabling infrastructures such as ICT. The use of ICT is therefore a welcome necessity that offers a platform for interconnectedness and efficient delivery of services.

Through this policy, the County Assembly of Kisumu intends to comprehensively offer a guidance to the effective uptake and use of ICT in all her service points. The policy shall help in ensuring prudence, efficiency and effectiveness thus reducing the turnaround time for all our services.

The County Assembly of Kisumu is aware that most public and private sectors are re-defining their policies and strategies to embrace ICT. In the public sector for example, the e- government strategy and the National ICT Policy were adopted in 2004 and 2006 respectively. Moreover, most County Assemblies have lately adopted the concept of e-parliament that heavily relies on ICT to operationalize the central functions of legislation, oversight and representation in parliaments across the world. In an effort to foster uptake of and full utilization of ICT, the County Assembly of Kisumu intends to establish medium and long-term ICT plan and adoption of an enabling ICT policy. There is also need to harmonize and integrate existing systems, present and future initiatives to the ICT systems. In this regard efforts to establish appropriate ICT standards, data security systems and procedures as well as related quality assurance mechanisms are a priority. In addition the Assembly will address the issue of staff capacity in ICT uptake.

This policy is therefore an immediate action plan that indicates the commitment of the County Assembly to implementing ICT in her operations. The Policy covers five crucial aspects of ICT as follows: Information Systems, ICT infrastructure, Human Resource, System Controls and security & Business Continuity.

1.2 Policy Rationale

The County Assembly of Kisumu procures and uses ICT systems and infrastructure in its operations. However, there is lack of a governing tool that can offer guidelines to ensure comprehensive access to, and utilization of ICT systems amongst staff and members of the Assembly. Moreover, the aspect of prudence in uptake of ICT systems and applications still remains a challenge. This has led to wastage and misuse of resources related to acquisition, repair and maintenance of ICT related equipment. These challenges can be attributed to little or limited information and guidelines on access and utilization ICT equipment. Moreover, these challenges are also aggravated by the low level of existing capacity amongst users within the Assembly in terms of technology.

This policy seeks to fill these gaps by offering ICT user guidelines and operationalization of ICT systems within the Assembly. The policy shall offer appropriate statements of ICT access, use, security and acquisition as well as business continuity in case of crises. The policy shall also increase the capacity of CAK to access data and process information necessary for improved service delivery.

1.3 Legal and Policy Framework

The policy derives its provisions from:

i. Constitution of Kenya 2010
ii. Kenya Information and Communication Act 2009
iii. E-Government Strategy;
iv. National ICT Policy;
v. Computer Misuse and Cyber Crimes Act 2018
vi. Access to Information Act 2016; and
vii. Any other relevant legal provision that may come into force

1.4 Objectives of the CAK ICT Policy

The objectives of CAK's ICT policy are to:

i. Support the development and implementation of ICT in The Assembly;
ii. Ensure development and maintenance of ICT systems;
iii. Promote efficient and effective operations and prudent usage of ICT systems within the Assembly;
iv. Facilitate the development of ICT skills to support ICT systems in the Assembly
v. Encourage innovations in technology development, use of technology and general work flows within the Assembly;
vi. Promote information sharing, transparency and accountability within the Assembly and towards the general public;
vii. Promote efficient communication among the Assembly's staff, Members and

stakeholders;

viii. Ensure that ICT facilities are fully accessible to users with special needs; and

ix. Ensure that ICT facilities are gender responsive.

1.5 Scope of the Policy

The ICT policy presents guidelines and policy information on all Information Technology facilities and services provided by CAK including, but not limited to, email system, databases, operating systems, internet, telephone systems, wireless communication, printers, scanners, copiers, biometric data capture and management systems, ICT process systems such as IFMIS, etc. All County Assembly members, staff, volunteers as well as business partners are expected to adhere to the provisions of this policy.

The policy shall be effective from the date of approval by the Board.

1.6 Key Principles

When implementing this policy, users shall be guided by the following principles:

i. Mainstreaming of ICT in the Assembly;
ii. Seamless integration of ICT;
iii. Inclusion, flexibility and support of other quality management systems;
iv. Adherence to best practices & policies;
v. Economies of scale and customer value propositions.

1.7 Roles and Responsibilities

The overall responsibility of implementing this policy will lie with the Clerk of the County Assembly of Kisumu in collaboration with HOD ICT and ICT Steering

Committee as is established in line with this policy.

2.0 ICT POLICY STATEMENTS/ GUIDELINES

2.1 Information Systems

i. This Information Systems policy is intended to support structured approach to acquisition, development, operations and maintenance of information systems in the Assembly.

ii. The head of ICT shall be the custodian and technical administrator of all Information Systems and Applications in the Assembly.

iii. All software acquired and developed shall be used strictly for CAK purposes only. Every software acquisition or development request shall be initiated through a written statement of scope and objective. The written statement will be submitted by the HOD ICT to the Assembly ICT Steering Committee and once approved will be submitted to the Clerk.

iv. **Acquisition of software:** With respect to software acquisition:

a. The Assembly will use packaged software as the preferred option;

b. In the event that custom development of software is proposed, the

request for such development must be justified on case by case basis;

c. Only open source software with technical support shall be used with approval by the head of ICT.

v. **Software application Development**: With respect to software application development:

a. Each software development project will be initiated on the basis of an approved requirements specification which:

b. Identifies user requirements (functional requirements) expressed in nontechnical language; Provide return on investment analysis;& Identifies beneficiaries.

c. If the Requirements (specifications) are approved the project sponsor and owner will proceed with the technical Specification to express user requirements specified in technical languages

d. The CAK shall purchase only fully licensed copies of computer software;

e. User testing and acceptance are the necessary and sufficient conditions for systems

vi. **Software Maintenance**: Application software maintenance is critical for effectiveness and efficiency of the system. The following policy will therefore apply:

a. Access to live systems will be restricted to authorized users;

b. Application software purchased must have service level maintenance agreements to ensure continuity;

c. Only CAK certified and pre-qualified and/or supplier authorized agents will be allowed to provide maintenance;

d. Internal maintenance shall be provided by personnel trained and certified; and

e. Maintenance contracts for Information systems in the Assembly shall be managed by the head of ICT.

vii. **System Decommissioning**: With respect to systems decommissioning:

a. All systems that will be commissioned shall have a predetermined life span;

b. At the end of the system life span, a review shall be done for the purpose of determining system usage, continuity or discontinuity;

c. For systems that have been in existence for five (5) years and above, a comprehensive review shall be carried out immediately this policy is effective;

d. For all newly acquired systems, a post installation review shall be carried out six(6) months after commissioning while subsequent reviews will be undertaken every two(2) years;

e. Systems that are no longer effective or in use will be decommissioned within 6 months after the review.

f. A Decommission Certificate will be issued on successful conclusion of the exercise;

g. Existing software will be replaced in the presence of a Certified Information Systems Auditor;

h. All copies of existing systems and data including source codes shall be placed in protective custody of the head of ICT for at least 15yrs.

viii. **Operating systems:** The following policies guidelines are intended to facilitate the governance of IT operating systems within the Assembly:

a. Microsoft's Windows Operating Systems will be the preferred Operating System for all computers.

b. The Assembly will standardize its office productivity tools on the Microsoft Office suite;

c. Commonly used functions that require the same templates will be supported through issuance of Assembly-specific templates.

d. Other operating systems like UNIX/LINUX may also be used on key equipment like servers if required.

ix. **Anti-virus software**: With respect to anti-virus software:

a. The head of ICT shall ensure availability and continuous update of anti-virus protection on all computers, laptops and servers

b. No person shall be allowed to connect private PCs, laptops, modems or any ICT peripheral to Assembly's network or hardware without authorization from the Head of ICT; and

c. All removable media in use within the Assembly must be scanned for viruses.

d. CAK will not be liable for loss of documents that are scanned and deleted by the anti-virus as a result of being found to be infected and cannot be cleaned.

x. **Data Management:** In order to ensure that data and information are available as and when required, the following policy statements will be adopted:

a. It is the responsibility of heads of functional areas in close consultation with the head of ICT to determine and design the data that should be available in the Assembly

b. The head of ICT will ensure overall data capture, availability, accuracy, confidentiality, and integrity.

c. The Assembly will acquire systems and tools to create, process, manage and preserve data;

d. The data shall be classified into Confidential and Public

xi. **Internet Based Systems:** The head of ICT will adopt and develop the following internet based systems as a means of communication and service delivery:

a. Web sites;

b. E-mail systems;

c. Short Message Services;

d. Intranet; and

e. Collaborative systems.

f. Shared Folders

2.2 Infrastructure

The objectives of Information Technology policies must be consistent with public sector standards and be in conformity with Parliament and other Assemblies. The policy must adhere to standards and guidelines and regulations of other bodies and E-Government policy.

2.2.1 Desktops, laptop computers, tablets, phablets and phones

(i) The Assembly shall seek to:

a. Standardize hardware equipment to minimize multi brands;
b. Allocate computers to user departments appropriately;
c. Provide uninterrupted power supply and protection to all ICT installations in order to protect the systems from power fluctuations and surges; and
d. Review hardware specifications to be in line with current technological trends.

(ii) Users are accountable for all ICT equipment allocated or assigned to them.

With respect to Laptops:

(iii) Laptops will be procured for service areas and assigned to officers whose nature of work merits their use;

(iv) Hardware specifications will be reviewed to be in line with current technological trends;

(v) Users are accountable for all laptops issued to them; and

(vi) There will be no additional software/ hardware installations without prior authorization from the Head of ICT.

2.2.2 Servers

The following best practices will be adhered to with respect to server deployments within the Assembly:

i. Maximization of the storage system;
ii. Ensuring online and offsite backups and real-time replication for critical applications;
iii. Disaster prevention arrangements (see Business Continuity)
iv. The acquisition of servers should be standardized to avoid multi brands;
v. All servers other than for backing up and disaster recovery shall be located in a central server room;
vi. The head of ICT will be responsible for the administration of all the servers in the CAK;
vii. Provide uninterrupted power supply and protection for all servers;
viii. Review hardware specifications to be in line with current technological trends.
ix. All servers deployed at CAK shall be configured according to the CAK security policies.
x. CAK shall allow authorized auditors, both internal and external, to access its servers to the extent necessary to allow them perform scheduled and ad hoc audits of all servers at CAK.
xi. Both Internal and external auditors shall never use access granted for any other purpose other than audit.
xii. Approved and standard configuration templates shall be used when deploying server systems.
xiii. Servers deployed at CAK shall be audited at least annually as prescribed by

and incompliance to applicable regulatory requirements.

2.3 Procurement of ICT hardware and software

The procurement of hardware, software, peripherals and network products shall be guided by procurement laws and regulations and:

i. Must conform to minimum specifications and standards established by the head of ICT;
ii. Must be informed by annual procurement plans.
iii. Take into account software requirements and anticipate future requirements;
iv. Be from manufacturers, authorized dealers and/or certified service center.
v. Must have warranty.

2.4 Inventory of ICT

i. The Assembly shall establish and maintain an inventory of all ICT equipment in the service areas.
ii. In the event of movement of officers occasioned by deployment or exit, the head of the affected service area shall reallocate any ICT equipment under their custody and communicate the same to the head of ICT, for purposes of updating the inventory. The equipment should be surrendered back to ICT department in case of exit of the user.
iii. Movement of ICT hardware from one office to another is restricted.

2.5 Installation, operations& Maintenance of ICT equipment

On installation of information technology products:

i. An Installation Certificate must be issued and signed by the head of ICT who shall be involved in the entire installation process;
ii. The head of the service area shall be responsible for all installations; and
iii. All installations must be in accordance with the supplier standards and Assembly requirements;

iv. All operations must have User and Technical manuals from the supplier;

v. The operating environment must conform to the minimum manufacturers' specifications or international standards; and Emergency procedures must be clearly displayed in the server room

vi. ICT hardware purchased must have Service Level Maintenance Agreements on expiry of the warranty;

vii. Only certified manufacturer authorized agents will be allowed to provide maintenance; and

viii. Internal maintenance shall be provided by personnel trained and certified.

ix. Maintenance contracts for ICT equipment shall be managed by the head of ICT.

x. The head of ICT shall develop maintenance schedule for all ICT equipment

2.6 Decommissioning and Disposal of ICT equipment

With respect to decommissioning ICT equipment:

i. All ICT equipment shall have a predetermined life span;

ii. There must be written justification by the head of ICT for decommissioning of any ICT equipment;

iii. Equipment that are no longer effective or in use will be decommissioned within 6 months after the review;

iv. ICT equipment will be decommissioned after an installation certificate has been issued for replaced systems;

v. A Decommission Certificate will be issued on successful conclusion of the exercise.

For purposes of disposal; Information technology resources disposal must:

vi. Be in accordance with the existing Public Procurement and Asset Disposal

Act 2015 and Regulations;

vii. Avoid or minimize degradation to the environment;

viii. Seek to re-use some of or all the computer components;

ix. Seek approvals of the Assembly in line with the Public Procurement and Asset Disposal Act 2015 to donate any retired computer equipment;

x. Remove data and systems on all hardware to be disposed off;

xi. Comply with manufacturer, supplier or service provider terms and conditions of disposal.

2.7 Useful life of ICT equipment

i. The useful life of desktop and laptop computers, tablets, phablets and phones will be 3 years. This means that it is only after this period that replacement, disposal, upgrade or decommissioning will be considered.

ii. Such replacement will be dependent on budgetary provisions and funds availability. Disposal of equipment that have reached the end of their useful life will depend on the operational status of such equipment.

iii. Disposal of equipment will be done as described under the disposal section of this policy and will be in line with the Public Procurement and Disposal Act together with supporting regulations.

2.8 ICT Human Resources

The human resource aspect of ICT is to ensure that the Assembly has personnel who are able to:

i. Provide effective and efficient support in the development and maintenance of ICT;

ii. Use ICT to support efficient and effective service delivery;

iii. Innovate and apply new technology consistent with ICT trends.

2.8.1 ICT Steering Committee

i. There shall be established an ICT Steering Committee for the County Assembly of Kisumu

ii. An ICT Steering Committee shall be charged with the responsibility of the overall strategic management of ICT resources in the Assembly. The Committee will be chaired by the Principle Finance Officer. The members will include selected heads of departments and the head of ICT as its secretary.

iii. Specific responsibilities for the ICT Steering Committee will include

a) Recommending, overseeing enforcement and reviewing the overall CAK ICT policy;

b) Providing direction and oversight in the implementation of the ICT strategy; and

c) Initiating and monitoring the implementation of ICT projects.

d) Planning, developing and approving ICT budget.

2.8.2 Capacity building

With respect to capacity building:

i. The head of ICT in consultation with the ICT Steering Committee will be responsible for the determination of overall ICT training needs and capacity building for CAS employees and agents;

ii. The Assembly will provide all employees with ICT skills and capabilities necessary for use of ICT resources;

iii. A skills development program consistent with the overall and strategic plan and Human Resource Development policy will be developed and implemented.

2.9 System Controls and Security

The Assembly's ICT systems, and the service they provide, will be protected by effective control of security risks at all levels of the organization, providing, managing and operating to ensure that the requirements regarding availability, confidentiality and integrity are preserved;

i. **Access:** Access to the systems will be restricted to authorized users as determined by the head of a service area.

ii. **Breaches:** Any breach of this policy shall be dealt with under the Assembly's Disciplinary Policy and Procedures. In addition, the Assembly may advise law enforcement agencies of the breach where it considers that a criminal offence may have been committed.

iii. **Review:** The Assembly will establish the ICT Steering Committee whose responsibilities will include the review of this aspect of the ICT policy from time to time and amended as need arises. Any changes shall be communicated to all users of the Assembly's ICT systems.

iv. **Physical Security**: *ICT* resources are generally exposed to the risk of unauthorized access, manipulation, disruption and natural disasters. In an effort to protect the ICT equipment and systems and ensure their availability the Assembly will institute appropriate control measures to ensure that its ICT resources are safeguarded. Appropriate controls will be established to limit access to *ICT* infrastructure, computer equipment and data, commensurate with the acceptable level of risk. The access to the Assembly's ICT systems shall be reviewed from time to time.

v. **Passwords:** The ICT section shall prevent unauthorized access to the Assembly's corporate computer systems. Such controls shall take the form of passwords in the user identification process. All ICT passwords shall be utilized and managed in line with basic standard password management criteria as shall be prescribed by the ICT department.

vi. **Data Security** : The head of ICT shall develop rules, regulations and guidelines that ensure confidentiality, integrity, availability and safety of all Assembly information.

3.0 COPYRIGHT AND LICENSE AGREEMENTS

Only licensed software shall be used in the Assembly. Copying and distribution should not be done without the necessary licenses. The head of ICT section will ensure that all software applications used by the Assembly complies with the relevant licensing agreements, compile all relevant licensing agreements and maintain a record.

4.0 EMAIL COMMUNICATION AND USE OF INTERNET

i. To ensure productive, appropriate use and to minimize risks, access to the Internet should be limited to official work. Users should use the Internet in an effective, ethical and in a lawful manner.

ii. Users should not use the Assembly's Internet access to view, print, distribute, display, send or receive images, text or graphics of offensive or obscene material or material that violates any Kenyan law.

iii. The Assembly shall maintain a log of sites visited as a means of determining appropriate usage.

iv. The Assembly shall install and maintain firewalls to filter content coming in or going out via the internet and protecting external attacks.

On Email communications;

v. The Assembly encourages the use of email and respects the privacy of users. The Assembly will not routinely inspect, monitor or disclose the contents of email without the consent of the user. However, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the Assembly may inspect, monitor, or disclose email when the Assembly believes that it has a business need to do so. The use of email must be related to the Assembly's business activities.

vi. For proper utilization of sever disk space, uncollected mails will be disposed after every forty five (45) days. Mail users will be allocated disk quotas of 500 MB for storing mail. Use of email is permitted as long as it does not:

a) Violate this policy

b) Degrade the performance of the network and

c) Divert attention from work

vii. A disclaimer shall be applied to all outgoing email

5.0 PRINTERS, TELEPHONE LINES, FAX AND COPIERS

i. Staffs are expected to use the above responsibly. Irresponsible/ excessive use of the above for personal purposes is discouraged, and may, depending on the ICT Manager's determination and management's approval lead to disciplinary action which may include, but not limited to, denial of the service.

ii. It is encouraged that printing of documents be done on both sides of the paper, "back- to-back", unless the document is for official use which prohibits back to back printing. This will ensure that there is less usage of stationery.

6.0 BIOMETRIC POLICY

i. The CAK shall use a Biometric Attendance System to monitor attendance of both staff and members in all relevant activities of the Assembly.

ii. Biometric Attendance Verification devices shall be installed at designated points in the Assembly to facilitate the monitoring process

iii. Assembly shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected.

iv. Biometric data will be deleted from the Assembly's Biometric Software systems promptly after a staff or a member's (MCA) relationship with the Assembly ceases, or when the initial purpose for collecting or obtaining such biometric data has been satisfied. In no situation will biometric data be retained for more than three years after staff or MCA's last interaction with the Assembly, unless otherwise required.

7.0 OUT-SOURCED ICT SERVICES

i. The Assembly shall out-source ICT Equipment and/or services whenever such capacity lacks in the Assembly with approval from the County Assembly Clerk upon recommendation from ICT Officer. Such a need shall be supported by a needs assessment report from ICT Officer.

ii. Acquisition of such services will be guided by the Public Procurement and Disposal Act (PPDA), 2015, and Public Procurement and Disposal Regulations (PPDR).

iii. All out-sourced ICT equipment and services will be supervised by ICT Officer in accordance with Service Level Agreements (SLAs) that are signed in consultation with County Assembly Clerk.

iv. The out-sourced services shall be based on annual contracts that may be renewed based on recommendations from the ICT Section.

8.0 OPERATIONAL CONTINUITY/ CHANGE MANAGEMENT PLAN

Major operational disruptions may pose a substantial risk to the continued operation of the Assembly. The extent to which the Assembly incorporates the risk of a major operational disruption in its continuity plan is dependent upon the institutional risk profile.

8.1 Change/ operational continuity plan

i. The Assembly shall ensure the implementation of the operational continuity/ change management plan by periodically conducting a operational impact analysis at least once a year.

ii. The County Assembly of Kisumu shall conduct an institutional risk assessment, risk management and risk monitoring to identify critical threats and risks associated with its activities and possible impact from major disruptions.

iii. The County Assembly shall provide sufficient human and financial resources to support Operational Continuity/ Change Management Plan.

iv. The County Assembly shall ensure adequate Back-Up of essential information and software in a comprehensive and well documented schedule.

v. Adequate back-up facilities shall be provided to ensure that all essential information and software can be recovered in case of a disaster, operational disruptions or media failure.

8.2 Responsibilities of the CASB and Management

i. The responsibility for business continuity management rests with the County Assembly Service Board and the senior management who are expected to formulate business continuity policy reviews, procedures and guidelines. All these must be documented and reviewed from time to time.

ii. The Board and senior management shall be responsible for:-

a. Institutionalizing Business Continuity Management Document;
b. Defining the roles and responsibilities for action in the event of a major disruption;
c. Constituting Business Continuity Management Team consisting of:
    (i) Coordinator (drawn from the senior management);
    (ii) Department Heads;
d. Constituting Crisis Management Team consisting of all heads of critical operational areas;
e. Accountability for business continuity management in cases of outsourced business continuity function.

8.3 Risk Assessment

i. A risk assessment examines the most urgent business functions identified during business impact analysis. It looks at the probability and impact of a variety of specific threats that could cause a business disruption.

ii. The Assembly shall undertake a Risk Assessment of its ICT processes from time to time

8.4 Business Impact Analysis

i. Business impact analysis forms the foundation upon which the business continuity plan is developed. It identifies critical business functions and operations that need to be recovered on a priority basis and establishes appropriate recovery objectives for those operations. It should be completed in advance of a risk assessment in order to identify the urgent functions upon which a risk assessment should be focused.

8.5 Recovery

i. The Assembly shall develop recovery procedures that reflect the risk they represent to the operation of its systems taking into consideration the interdependency of risks.

ii. The Assembly shall facilitate testing of plans to ensure that crisis and recovery teams are aware of their roles and responsibilities in the event of a disruption.

iii. In cases where the Assembly shares or outsources a disaster recovery site, there must be service level agreements or contract in place that clearly outline the terms that govern these arrangements between the parties.

iv. Recovery solutions must be based on Business Impact Assessment (BIA) information.

9.0 GENERAL USE, ACCEPTABLE USE AND OWNERSHIP

i. Users of CAK's network should be aware that the data they create on the corporate systems remains the property of CAK and management cannot guarantee the confidentiality of personal information stored on any network device belonging to CAK.

ii. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Any information that users consider sensitive or vulnerable should be encrypted.

iii. For security and network maintenance purposes, authorized individuals within CAK may monitor equipment, systems and network traffic at any time, in accordance with CAK's Internal Audit Policy. CAK reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

iv. The ICT Department shall monitor and report internet use from all computers and devices connected to the corporate network in accordance to the Internet Security Policy.

v. The ICT Department shall block access to Internet websites and protocols that are deemed inappropriate for CAK's corporate environment. Websites with the following contents should be blocked: Adults only/Sexually Explicit Material, Advertisements and Pop-Ups, Gambling, Hacking, Illegal Drugs, Dating, SPAM, Phishing and Fraud, Spyware and Malware, Violence, Intolerance, Hate and Terrorism

vi. Under no circumstances is an employee of CAK authorized to engage in any activity that is illegal under Kenyan or international laws while using CAK - ICT resources. The following activities are, in general, prohibited. Employees may be exempted from these restrictions in the course of their legitimate job responsibilities (e.g., systems administration employee may have a need to disable the network access of a host if that host is disrupting production services).

vii. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CAK.

viii. Unauthorized copying of copyrighted material including, but not limited to, digitization

and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CAK or the end user does not have an active license is strictly prohibited.

ix. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

x. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)

xi. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

xii. Using CAK computing assets to actively engage in procuring or transmitting material that promote sexual harassment or hostile workplace laws.

xiii. Making fraudulent offers of products, items, or services originating from any CAK account.

xiv. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

xv. Circumventing user authentication or security of any host, network or account.

xvi. Providing information about CAK or its employees to third parties without authorization

10.0 MONITORING AND EVALUATION OF ACCEPTABLE USE OF ICT

i. Intranet, Extranet and Internet related systems, including webmail, computer equipment, software, operating systems, storage media, network accounts, CAK website, online portal and database servers, are the property of CAK and therefore should be used for work related purposes. Inappropriate use exposes CAK to risks such as virus attacks, compromise of network systems and services as well as litigation.

ii. All ICT systems and equipment are the property of the County Assembly of Kisumu. The Assembly therefore reserves the right to monitor these systems to ensure compliance with this policy. The monitoring of the ICT system activities will be carried out in a manner that respects the rights and legitimate interests of those concerned.

iii. Users of the Assembly's ICT systems should be aware that their activities can be monitored and they should not have any expectation of privacy. In order to maintain their privacy, users of the Assembly's ICT resources should avoid storing information on these systems that they consider private. By using the Assembly's ICT systems, users expressly consent to the monitoring of all their activities within the Assembly's ICT systems.

iv. During the implementation of this policy, the Assembly will ensure that there is continuous monitoring and evaluation for efficiency, accountability and transparency. The Monitoring and Evaluation will be carried out by the ICT internal M&E team in consultation with the CAK Steering Committee.

11.0 COMPLIANCE

All users of the Assembly's ICT systems are required to read the ICT security policy and give a written declaration that they will adhere to the guidelines set out in the document. The signed declaration should be returned to the head of ICT. A

simple declaration sent on mail shall be deemed sufficient.

12.0 POLICY REVIEW

This policy will be reviewed after every five (5) years and or as of when need arises as maybe approved by the Board.

APPROVAL

POLICY TITLE:	County Assembly of Kisumu ICT Policy
POLICY RATIONALE:	To outline guidelines for effective, efficient and prudent acquisition, utilization and maintenance of ICT systems and infrastructure within the County Assembly of Kisumu
POLICY CONTACT:	Head of ICT Department
APPROVAL AUTHORITY:	The County Assembly of Kisumu Service Board
COMMENCEMENT DATE:	

SIGNED: _____ SEPT, 2022

Clerk of County Assembly of Kisumu **Date**

_____ SEPT, 2022

Chairperson of County Assembly **Date**

Service Board

Prepared By:
Office of the Clerk
County Assembly of Kisumu
P.O Box 86 - 40100, Kisumu, Kenya
Email address: clerk@kisumuassembly.go.ke
www.kisumuassembly.go.ke
info@kisumuassembly.go.ke

LOCATION

The County Assembly of Kisumu is located in Kisumu County, Kisumu Central Constituency, Kisumu City: VQW+753, Uhuru Rd, Kisumu. We also have operational ward offices (Office of the MCA) in all the 35 wards in Kisumu County.

Official working Hours

Monday - Friday between 8:00am and 5:00pm. Closed on public holidays and weekends.

All feedback on our services should be channeled through:

Office of the Clerk
County Assembly of Kisumu
P.O Box 86 - 40100, Kisumu, Kenya
Email address: clerk@kisumuassembly.go.ke
www.kisumuassembly.go.ke
info@kisumuassembly.go.ke

Feedback form is available and can be filled and submitted online through our website