COUNTY GOVERNMENT
OF BUNGOMA

COUNTY ASSEMBLY OF BUNGOMA

INFORMATION, COMMUNICATIONS AND TECHNOLOGY (ICT) POLICY & MANUAL

December, 2022

COUNTY ASSEMBLY SERVICE BOARD

Table of Contents

FOREWORD

Information Communication and Technology (ICT) Policy provides a roadmap to ICT implementation strategies.

The County Assembly of Bungoma takes cognizance of emerging risks and threats such as cyber-crime and misuse of computer technology. It has incorporated technology in most of its operations and is progressively moving towards full digitalization and automation of key services.

We have put measures in place to ensure business continuity through ICT Disaster Recovery Plans, Computer Security, Cyber Security and Information Security in the protection of computer systems and networks from theft or damage to the hardware, software, electronic data and from the disruption or misdirection of the services provided by the institution.

The policy provides a framework for streamlining the ICT sector and enhancing its ability to catalyze execution of the mandate of the County Assembly namely legislation, representation and oversight.

This Policy provides important control and governance tool necessary at this time of information-age where an organisation's data is such a critical asset. It will also help members of staff improve their capacity to perform duties.

This policy is addressed to all County Assembly staff and it should be complied to and its guidelines followed in the County Assembly.

Hon. Emmanuel M. Situma
Chairperson, County Assembly Service Board

PREFACE

ICT Policy *promotes fair use of ICT resources and provides guidelines on acceptable usage of* network equipment and computing systems.

The Policy Guidelines has objectives which cover: ICT *Infrastructure Development; Facilitation* of Infrastructure and Frameworks Development; development and maintenance of ICT systems, efficiency and effective operations; and usage of ICT systems, development of ICT skills to support ICT systems and innovations in technology development.

Its successful implementation will position the County Assembly to take advantage of the emerging trends by enhancing its operations and further result into innovation, efficiency and quality in public service delivery.

The implementation of this Policy will enable the County Assembly to carry out its mandate in a more professional, efficient and effective manner. All employees are, therefore, expected to embrace the use of ICT in their day to day operations. It is my hope that the Policy will guide the employees in providing quality services to the Customers and Stakeholders

This policy applies to all Members of the County Assembly and staff.

Charles W. Wafula
Secretary, County Assembly Service Board

ABBREVIATIONS AND ACRONYMS

BCP	-	Business Continuity Plan
BYOD	-	Bring Your Own Device
CCTV	-	Closed Circuit Television
CIRT	-	Computer Incident Response Team
CIT	-	Contract Implementation Team
CRM	-	Customer Management System
DR	-	Disaster Recovery
DRP	-	Disaster Recovery Plan
EDMS	-	Electronic Document Management System
HRMIS	-	Human Resource Management Information System
ICT	-	Information Communication Technology
ISMS	-	Information Security Management System
LAN	-	Local Area Network
NDA	-	Non-Disclosure Agreement
NEMA	-	National Environment Management Authority
OLA	-	Operational Level Agreement
OSHA	-	Occupational Safety and Health Act
PPRA	-	Public Procurement Regulatory Authority
SCMS	-	Supply Chain Management Services
SLA	-	Service Level Agreement
SOP	-	Standard Operation Procedures
UPS	-	Uninterrupted Power Supply
WAN	-	Wide Area Network
WLAN	-	Wireless Local Area Network
VESDA	-	Very Early Smoke Detection Apparatus

CHAPTER ONE

1.0. INTRODUCTION

1.1 Background Information

The County Assembly of Bungoma encourages the use of electronic communication to share information and knowledge in support of the County Assembly of Bungoma's mission and vision. To this end, the County Assembly of Bungoma supports and provides interactive electronic communication and services and facilities such as telephones, teleconferencing, video conferencing; electronic mail, bulletin boards, social networking; electronic publishing services such as internet. These communication services rely on underlying voice, video, and data networks delivered over both physical and wireless infrastructures. Digital technologies are unifying these communication functions and services.

In 2022, the County Assembly of Bungoma adopted a ten-year strategic plan (2022-2031) that outlined its overall vision, mission as well as other ways to improve delivery of ICT services. One of the areas that the County Assembly of Bungoma is giving considerable attention is in the formulation and implementation of an ICT policy and strategy. The County Assembly of Bungoma is aware that most institutions in both public and private sectors are re defining their policies and strategies to embrace ICT. The immediate challenge for the County Assembly of Bungoma is to establish short, medium and long-term ICT plan adoption of an enabling policy. There is need to harmonize and integrate existing systems, present and future initiatives. In this regard, efforts to establish appropriate ICT standards, data security systems and procedures as well as related quality assurance mechanisms are being put in place.

The policy recognizes this convergence and establishes an overall policy framework for electronic communication. This policy clarifies the applicability of laws and of other County Assembly of Bungoma policies to electronic communication. The purpose of this policy is to provide a framework within which all the new issues that might arise in electronic communication can be resolved.

1.2. Policy statement

The County Assembly of Bungoma is committed to creating an enabling environment for promotion and use of ICT in the provision of services in a manner that is ethical, efficient, effective and lawful. The Assembly will continuously enhance its organizational capacity by adopting modern technology and skills development.

1.3 Context Rationale

The dynamic nature of technology and the significant continued absorption of ICT use in the county assembly to improve service delivery calls for the review of its ICT Policy 2016 to resonate with these requirements. Rapid technological changes, changing public needs, legal framework and evolving ICT global trends require a policy to provide a suitable anchor. In order to provide a clear guidance on the acquisition, development and use of the ICT resources in the Assembly while offering the required protection to the Assembly Information Assets, it was necessary to develop this policy.

CHAPTER TWO

2.0 POLICY FRAMEWORK

2.1. Strategic Direction

The vision of this policy will guide the implementation of the communication functions towards ensuring information provision, awareness raising and understanding. This will ultimately encourage the participation of the County Assembly citizenry in the timely, effective and responsive delivery to services by an accessible and accountable leadership.

2.2 Policy Objectives

The objectives of County Assembly of Bungoma's ICT policy are to:

1. Ensure development and maintenance of ICT systems.
2. Support development and implementation of ICT in the County Assembly of Bungoma
3. Promote efficiency and effective operations; and usage of ICT systems within the County Assembly of Bungoma.
4. Facilitate the development of ICT skills to support ICT systems in the County Assembly of Bungoma
5. Encourage innovations in technology development, use of technology and general work flows within the County Assembly of Bungoma
6. Promote information sharing, transparency and accountability within the County Assembly of Bungoma and towards the general public
7. Promote efficiency communication among the County Assembly of Bungoma's staff, customers and/or stakeholders.
8. Ensure that ICT facilities are fully accessible to all MCAs and staff

2.3 Scope

This Policy applies to all Users (Members of County Assembly, employees, ICT suppliers, contractors and service providers).

2.4 Policy Principles

The Policy shall be guided by the following key principles:

(i) Seamless integration of ICT systems.

(ii) Adherence to international ICT standards and best practices.

(iii) Security, integrity and reliability of data and information systems.

(iv) Transparency and accountability in service delivery.

(v) Innovation and ease of doing business.

(vi) Inclusion, flexibility and support of other quality management systems

(vii) Economic scale and customer value propositions

2.5 ICT Governance

The ICT Strategic Committee at the Board Level, should be responsible for Information Communication Technology (ICT) Governance. ICT governance can be considered as a framework that supports effective and efficient management of ICT resources to facilitate the achievement of the institution's strategic objectives.

The ICT Steering Committee shall be responsible for ICT strategic decisions to ensure that all ICT projects and initiatives deliver value to the organization. The committee shall use E-governance guidelines.

The ICT Steering Committee will be bounded with the responsibility for the overall strategic management and monitoring of ICT resources utilisation and key ICT projects progress in the organisation shall be established.

The responsibilities of these Committees are as indicated below**.**

2.6 ICT Committees

2.6.1 ICT Strategic Committee at the Board

The ICT Strategic committee at the Board shall be established by the board.

General Objective

To assist the Board in reviewing and overseeing the overall ICT governance of the Institution.

1. Appointment & Membership

a. The ICT Strategic Committee is a Committee of the Board, duly constituted as per the County Assembly Services Act, 2017

b. The number of members shall be determined by the Board from time to time

c. When making the appointment the Board will ensure that:

i. At least one of the members has expertise in Information Technology

ii. Every member appointed is familiar with the ICT strategic Committee's

terms of reference.

iii. Every member appointed is aware of the interest of all stakeholders.

2. Roles and Responsibilities

The ICT Strategic Committee shall as a minimum ensure sound ICT governance, including:

a. Ensuring that an ICT governance charter and policies are established and implemented. The charter and policies should outline the decision-making rights and accountability framework for ICT governance that will enable the desirable culture in the use of ICT within the Assembly.

b. Oversee the cultivation and promotion of an ethical ICT governance and management culture and awareness. The Committee should provide the required leadership to achieve this institution‘s strategic objective.

c. Ensure that an ICT internal control framework is adopted and implemented and that the board receives independent assurance on the effectiveness thereof. The necessary steps should be taken to ensure that there are processes in place to ensure complete, timely, relevant, accurate and accessible ICT reporting.

d. Ensure that the ICT strategy is integrated with the institution‘s strategic and business processes. ICT should be seen to add value by enabling the improvement of the institution‘s performance and sustainability.

e. Consider the suitable strategy, structure and size of the ICT function, considering what is appropriate for the adequate management of the ICT function and associated risk of the institution and having regard to any legislative requirements that apply to the ICT function. The structure of the ICT function, its role and its position in terms of reporting lines, should reflect the Assembly‘s decision on how ICT is integrated with its operations.

f. Oversee the proper value delivery of ICT and ensure that the expected return on investment from significant ICT investments and projects is delivered and that the information and intellectual property contained in the information systems are protected.

g. Where the responsibility for the provision of ICT goods or services has been delegated to another party (or division), the Committee to remain accountable for enforcing and monitoring effective ICT governance. Ensure that Management regularly demonstrates to the board that the institution has adequate business resilience arrangements in place for disaster recovery and business continuity.

3. Specific Duties

In carrying out the responsibilities conferred upon the Committee in 2 above, the ICT Strategic Committee will have the following specific duties at an oversight level:

Strategic Alignment

a. Periodically review ICT Strategy and ensure it is aligned with business strategy.

b. Evaluate Management Reports on benefits delivered by ICT projects (benefits realization)

c. Issue high-level policy guidance to communicate goals and objectives

d. Periodically review Management reports on industry trends.

e. Review Management prioritization and allocation of resources to ensure delivery of the ICT Strategy.

f. Manage and oversee a rolling five-year investment programme.

4. Value Delivery

a. Review ICT related expenses towards optimization.

b. Ensure there is in place a methodology to evaluate Return on Investment (ROI), which ensures there exists a balance between risks and benefits.

5. Resource Management

a. Consider Business Cases for all ICT enabled investment decisions of strategic importance.

b. Ratify all ICT procurements

c. When agreed, monitor delivery of all ICT-enabled projects of strategic importance.

d. Through Management reports or Independent reviews, ensure that ICT has competent, sufficient and efficient resources: applications, information, infrastructure and personnel.

e. Provide high-level direction for sourcing and use of ICT resources (e.g. strategic alliances).

5.1 Risk Management

a. Receive assessment and reports on ICT-related risks and organization impact.

b. Through Management reports, ensure that there is in place, a Business Continuity Plan (BCP) to include disaster recovery and continuity of operations.

c. Ascertain that risk management is embedded in the ICT operations.

5.2 Performance Management

a. Ascertain there exists a methodology and tools for Management to track project completion, process performance and service delivery, as well as resource usage and monitoring of ICT Services.

b. Ensure a Balanced Score Card (BSC) is in place for ICT.

c. Through Management reports, verify strategy compliance.

6. Additional duties

a. Review the Committee’s terms of reference at least once every three years and recommend modifications.

b. Carry out other tasks, special assignments and investigations as may be requested from time to time by the Board.

c. Consider any matter of significance pertaining to ICT raised at the Audit and risk management committee meetings.

2.6.2 ICT Steering Committee

1. **Establishment**

   An ICT Steering Committee shall be established by the accounting officer.

2. **Responsibilities**

   The Committee shall be responsible for overseeing the development, implementation and monitoring of the ICT policy, strategy, projects prioritization, execution and governance matters. In undertaking these responsibilities, the committee may:

i. Recommend projects of strategic importance in line with the Assembly's Strategic Plan and ensure a strategic balance.

ii. Review project risks including; Disaster, Audits and advisory on ICT related projects.

iii. Co-ordinate ICT project prioritisation based on programme priorities to inform the Assembly's planning and budget cycle, provide regular reports and present business case budgets and priorities for strategic ICT projects to Assembly Board Committees.

iv. Recommend action, including the suspension of projects.

v. Develop annual Cycle of ICT Governance business which includes: discussion on emerging strategic ICT issues; regular review and approval of the Assembly's ICT risk register; review of reports from the ICT department on Assembly's ICT business continuity and disaster recovery plans and procedures and review reports on ICT security.

vi. Review reports on ICT related items identified by internal or external audit reports to ensure timely resolution.

vii. Review and lead continuous improvement on ICT Governance matters across the Assembly.

2.6.3 Invitees

The Committee may invite any person or persons to its meetings as it may determine to assist in its deliberations either on a particular item or for the whole meeting.

2.6.4 Reporting

The committee reports to the Management committee.

2.6.5 Review of the Committee

The committee will review its functions and performance yearly.

2.6.6 Frequency of Meetings

The ICT Steering Committee will meet at a minimum four (4) times a year with at least one meeting in each quarter.

Meetings will generally be scheduled at least one quarter in advance to align with the Assembly's planning cycle.

2.6.7 Quorum

The quorum for meetings of the ICT Steering Committee is a half of the membership with prior-approval from the Chairperson.

2.6.8 Decisions

Decisions shall be through consensus.

CHAPTER THREE

3.0 ICT Infrastructure

The County Assembly of Bungoma may establish and continuously improve standards on installation, security, management, use and implementation of ICT infrastructure in all service delivery points/locations. The guidelines shall address four (4) key areas namely; ICT networks, ICT facilities, power provisions and equipment as provided below:

Guidelines for ICT Infrastructure

1. *Network Management*

The network shall be set up in all Assembly offices and managed in adherence to the standards outlined in the following guidelines:

i. The network shall consist of the Local Area Network (LAN), Wide Area Network (WAN) and Wireless Local Area Network (WLAN).

ii. Emphasis shall be on the adoption of secure networks in deployment of the network infrastructure.

iii. The devices in the network ecosystem shall include but not limited to; computers, devices that support the flow and processing of information, ICT data centre, telephone systems and related software.

The ICT department shall: -

i. Maintain a clear network layout diagram of all Assembly premises for purposes of reference, maintenance, support, expansion and business continuity.

ii. Monitor the utilisation of the network infrastructure and advise on future expansion and security, in line with international standards and best practices.

iii. Periodically review technical specifications, configuration and installation guidelines to ensure conformity and compatibility with existing infrastructure.

iv. Only approved network connectivity devices by the ICT department shall be allowed to transmit signals to connect the Assembly equipment within the Assembly premises.

v. Access to Assembly server rooms and network cabinet installations shall be

restricted to Authorised personnel.

vi. The Assembly reserves the right to monitor internet usage and block sites or users to ensure security and integrity of its data assets and any other resources.

2. *ICT Facilities*

ICT facilities include; the server rooms, data centres, operation rooms and any other room dedicated to ICT infrastructure and equipment in the County Assembly.

The following guidelines shall apply:

i. All infrastructure projects including new construction and refurbishment shall include approved designs for ICT installation as part of the scope of works for the projects.

ii. Data centres shall house all servers' core network equipment and shall be provided with uninterrupted power supply (UPS), air conditioning, Very Early Smoke Detection Apparatus (VESDA), Fire Suppression, CCTV Monitoring, Humidity and Water Monitoring Instrument and Access Control and Notification Systems.

iii. Equipment rooms and locations shall have Network cabinets and associated

equipment necessary for distribution of Assembly network.

iv. There shall be facilities to house Major Uninterrupted Power Supply (UPS) equipment.

v. ICT facilities shall be optimally located within the Assembly premises. Such a location shall consider factors including but not limited to security, fire resistance, noise, heat and electricity supply.

3. *Power Provision*

ICT facilities and equipment require stable power provision to prevent failures or inaccessibility of online services.

The following guidelines shall apply:

i. The ICT department, in consultation with the responsible implementing unit (s), shall ensure that Assembly offices are installed with adequate backup power supply.

ii. All active critical ICT infrastructure shall be connected to clean power.

iii. All users/process owners shall seek authorisation from designated ICT Officers to alter, repair or replace ICT equipment.

iv. The UPS shall be used to power ICT equipment only.

v. Other electrical appliances such water dispensers and electric fans shall only be connected to regular power.

4. Management of ICT Equipment

These guidelines apply to specifications, requisition, procurement, allocation, distribution, asset register, maintenance, use and disposal of ICT equipment in the Assembly. All equipment remains the property of the County Assembly of Bungoma and users **must** take care of the equipment under their custody and use.

a) Requisition

i. The requisition for all ICT equipment and accessories shall be made by the respective Heads of department or Sections through the ICT department.

ii. The ICT department shall from time-to-time review and consolidate such requisitions, confirm they are required and prepare technical specifications and requirements for each item.

b) Acquisition

The ICT equipment may be acquired through purchase or donations.

i. The procurement and delivery of ICT equipment shall be guided by existing laws and government procurement regulations. Acquisition of ICT facilities shall be guided by the provisions of the Public Procurement and Asset Disposal Act, (PPDA) 2015, Public Procurement and Asset Disposal Regulations (PPDR) 2020, Best Practices and the County Assembly of Bungoma Procurement Manual. Where funds are donated from external sources, the respective donor conditions, terms, agreements or memoranda of understanding shall apply.

ii. Donated ICT equipment shall be accepted upon meeting minimum specifications or on advice by the ICT officer.

iii. ICT goods, related services and/or works once acquired will be received by the County Assembly Inspection and Acceptance Committee in line with the Public Procurement and Asset Disposal Act (PPDA), 2015 and the Public Procurement and Asset Disposal Regulations (PPDR), 2020 framework. The Committee shall seek professional assistance from the ICT department.

c) Disposal

i. The ICT department shall identify hardware and software to be disposed and liaise with Procurement department for assessment leading to disposal as per the PPDA, 2015 and the PPDR, 2020.

ii. The ICT department shall ensure that all equipment earmarked for disposal is cleared of Assembly data and storage media destroyed.

d) ICT equipment asset register

The ICT department shall maintain an ICT asset register for monitoring the issuance, usage, surrender, movement, maintenance and loss of ICT equipment acquired by the Assembly.

i. The register shall contain details of all ICT equipment.

ii. The ICT officers shall conduct quarterly inventory audit of the equipment and submit a report to the HOD.

iii. The equipment that is no longer in use shall be surrendered to the ICT department for redistribution or recommendation for disposal.

e) Allocation and responsibility

i. The ICT equipment shall be allocated to an individual employee in accordance with the ICT Equipment Allocation Matrix **Annex I**.

ii. The ICT department shall ensure that ICT equipment issued to staff match the nature of their work.

iii. The user issued with an ICT equipment shall fill the ICT Equipment Acknowledgement Form.

iv. The ICT department shall ensure that all ICT equipment are standardised for ease of maintenance

v. Users who require specialized equipment shall submit a written request to the ICT department for advice and consideration.

vi. Members of staff issued with new or replacement of equipment shall surrender the old one immediately after inspection by the ICT officer for update of the inventory.

vii. The ICT department and users shall ensure that data from the surrendered machine is backed up or transferred to new equipment where necessary.

f) Issuance of ICT equipment

i. Members of staff to be issued with ICT equipment shall be required to sign the ICT Equipment Issuance Form from ICT department.

ii. All staff shall be responsible for equipment issued to them.

iii. Non-employees of the County Assembly are prohibited from using ICT equipment.

g) Custody of ICT equipment

i. The custody of all ICT equipment shall be done in collaboration with the Supply Chain Management Services section under the guidance of the Clerk.

ii. The ICT equipment shall only be moved from the current station with the authority of the HOD after filling the ICT Asset Movement Form.

iii. An Employee on secondment to other institutions shall surrender all equipment in their possession as prescribed in the clearance procedure of the Human Resource Manual.

h) Security and loss of ICT equipment

i. Necessary precaution shall be taken while using ICT equipment out of the Assembly premises. Failure to demonstrate due diligence in protecting equipment shall constitute negligence and the user shall be held liable for the loss.

ii. Loss of ICT equipment must be reported immediately to the nearest police station and an abstract obtained. Thereafter, the loss must be reported to the Clerk using the ICT Lost-Damaged Equipment Reporting Form.

iii. The ICT department shall regularly carry out awareness on information security.

iv. All employees must be aware that any loss of data held in ICT equipment exposes the Assembly to serious security lapses. All necessary measures must therefore be taken to protect the data in the devices.

i) Maintenance of ICT core infrastructure

i. Manufacturers' warranties shall be diligently managed for core ICT infrastructure. Maintenance contracts and Service Level Agreements shall be in place for core equipment at all times.

ii. The ICT department shall perform scheduled maintenance of core ICT infrastructure.

iii. The ICT department shall prepare a technical report with recommendations for decommissioning non-performing core ICT infrastructure in readiness for disposal.

j) Acceptable use of ICT infrastructure

Acceptable use of ICT infrastructure entails appropriate and responsible use of such facilities in the dispensation of Assembly Services. The following guidelines shall apply:

i. ICT infrastructure shall not be used for personal activities.

ii. Unauthorised connection of monitoring devices/equipment to the Assembly ICT infrastructure is prohibited.

k) Provision of Internet Services

The following guidelines shall apply in the provision of Internet Services:

i. The Assembly shall provide Internet Services and resources to facilitate service delivery.

ii. The Internet Services and Resources shall be exclusively used for the County Assembly service delivery.

iii. The Assembly reserves the right to monitor internet usage.

The user shall not use the internet for;

i. Personal use or gain.

ii. Disseminating or printing copyrighted material in violation of copyright laws.

iii. Carrying out activities that could cause congestion and disruption of Assembly network and systems.

iv. Inappropriate and unlawful content.

The use of the internet shall conform to the Assembly Code of Conduct and Ethics. The Assembly reserves the right to provision of internet utility which is also subject to budgetary allocation. The Assembly reserves the right to block sites and users from internet access as it may deem appropriate.

l) ICT Information Systems

The County Assembly of Bungoma shall provide guidelines on the acquisition of appropriate software in terms of use, value for money, scalability and integration with existing and future systems in the Assembly. The systems will be used, operated and managed efficiently to ensure effective service delivery. The detailed guidelines are as indicated below.

m)Information Systems

The County Assembly Information Systems are implemented for the sole purpose of improving the effectiveness and efficiency of service delivery. These Information Systems may have major impact on corporate strategy and organisational success. Thus, require involvement of the management in all aspects.

n) Information Systems Development

The development of Information Systems for the Assembly will follow the approved open standards and methodology.

o) Information System Database and Backups

The Assembly data is very critical in decision making hence, the need to ensure the data repositories are secured and backed up for restoration in case of disaster or logical errors. The Assembly shall backup its information systems and databases.

General Requirements

The Assembly shall:

i. Determine whether to develop or acquire a required Information System(s).

ii. Ensure that the Information System is operational, well maintained and sustainable.

iii. Ensure all software is strictly used for the Assembly's purposes only.

iv. Ensure the Information Systems meet approved quality standards.

v. Ensure process owners consult with the ICT department on matters relating to;

   a) Integration of ICT in their processes.

   b) Implementation of specific components of the ICT Policy and Strategy that support their processes.

   c) Compliance with the ICT Policy.

vi. Establish a strategy for managing changes in the Information System for new deployment.

p) Information Systems Acquisition

The following procedure shall apply in the acquisition of ICT Information Systems:

i. Acquisition and or applications shall be done in accordance with the provisions of the relevant procurement law.

ii. A detailed business and system requirement shall be established before any application or acquisition.

iii. Specifications shall be developed to guide in the selection of competent suppliers.

iv. The operating environmental conditions must conform to the minimum

manufacturers' specifications and best practices.

v. Capacity building and transfer of knowledge of deployed Information System shall be conducted by the supplier before a completion certificate is issued.

vi. Process owners shall be involved in the acquisition, implementation of new systems and training of staff upon installation. User acceptance shall be provided for all new Information Systems installed.

vii. Ensure compliance with best practice for any system being acquired.

viii. Upon successful installation of any Information System, a completion Certificate duly signed by the Clerk shall be issued.

ix. User and Technical Manuals shall be part of the minimum requirements for all systems acquired or developed by the Assembly.

q) Information Systems Development

The following guidelines shall apply in the development of Information Systems in the Assembly:

i. Information Systems developed in-house shall be a property of the Assembly.

ii. The platform and database to be used shall be approved by the ICT department.

iii. The ICT department shall ensure that backup and recovery procedures for each system are documented and periodically reviewed.

iv. System design must be approved by the ICT department and the process owner before a system development.

v. Final system source codes shall be surrendered to the Assembly through the head of department.

vi. System codes, configurations data and installation kits shall be backed up.

r) Information Systems and Software Maintenance

Information System and Software Maintenance include any activity which requires use of an information system for the purpose of upgrading, reconfiguring, modifying, replacing, changing or servicing within a given period of time. Maintenance includes, but not limited to software changes, hardware changes, patches, fixes and updates.

The following guidelines shall apply:

i. The ICT department shall advise the Assembly on Information Systems and Software Upgrades.

ii. Information Systems and Software shall be maintained regularly to ensure compliance with the changing requirements of the Assembly and technological changes.

iii. New Information Systems and Software shall be installed and tested in the test environments based on the information systems testing procedure as indicated in (Information Systems Testing).

iv. A System Change Request Form shall be filled, duly signed and approved for any change to be effected.

v. The System Administrator shall schedule systems maintenance at an appropriate time with a prior notice and approval from the Clerk though the head of department accordingly.

vi. Applicable system maintenance logs and documentation shall be updated and reviewed after maintenance.

s) Information Systems Testing

The following guidelines shall apply in the testing of an Information System:

i. Different aspects of the System shall be tested such as, response to time, boundary data, no input and heavy volumes of input.

ii. The programmer who develops the system will not be the one to perform the testing.

iii. Standard debugging tools shall be used.

iv. A Test and Quality checklist shall be maintained indicating the test results.

v. The process owner shall be involved in the testing of the system.

t) Information Systems Documentation

The following guidelines shall apply in the documentation of Information Systems:

1. Every Information System shall have the following documents;

    a) System Documentation.

    b) User Manual.

    c) Training Manual.

2. The standard for the documentation shall be comprehensive, informative and well structured.

u) Information Systems Monitoring and Evaluation

i. ICT department together with the process owners shall conduct monitoring and evaluation of systems after every two (2) years to determine areas of improvement on all systems.

ii. User satisfaction survey shall be conducted annually to establish success of the Information Systems.

v) Information Systems Decommissioning

The Assembly shall ensure that all systems commissioned have a predetermined lifespan. A review shall be done in every two (2) years to determine the system usage, continuity, discontinuity or decommissioning.

At the end of life, a changeover or replacement, the Information System shall be decommissioned. When decommissioning a System, the Assembly shall ensure that existing data is protected and stored for future use and made available as required.

The following guidelines shall apply:

i. A System shall be analysed for its usefulness and need.

ii. Once an Information System, Application and/or Database reaches its end-of-life, a Service Area may seek to decommission the System, Application and/or Database by making a formal request to the Clerk through HOD.

iii. When decommissioning an information System, Application and/or Database, records retention policies may require that the records contained within the information System, Application and/or Database be retained beyond the useful life of the Information System, Application and/or Database.

iv. There shall be a last backup done as per the Systems Backup Guidelines.

w) Software

The following guidelines shall apply to all Software in the Assembly:

i. Establishment of appropriate Software Standards to facilitate acquisition and development.

ii. Approval of the Software by the ICT department prior to acquisition, download, installation and use is required. Any Software serving a specific Service Area, the process owner shall, together with the ICT officer issue the approval.

iii. Proprietary Software must be licensed throughout their life and where necessary supported.

iv. Open Source, Shareware or Freeware Software must be compatible with the Assembly's Hardware and Software Systems.

v. Assembly users shall use Software in conformity to copyright laws, terms of licensing and use.

vi. The Assembly shall endeavor to use Software that do not require licensing or use one-off licensing and use Open Standard Architecture.

x) User Accounts

The following guidelines shall apply for employees' user accounts:

i. Employees shall make formal requests for a user account by filling the System Access Request Form. The form shall be recommended by their immediate Head of department and approved by Clerk.

ii. User accounts shall be uniquely created.

iii. User accounts that are unused shall be disabled.

iv. Users shall be granted privileges that are commensurate to their roles and responsibilities.

v. All other users but not limited to contractors, vendors, attachees and interns can be given access at the discretion of the Clerk.

y) E-mail Services

The following guidelines shall apply for E-mail Services:

i. All official communication shall be done through the county assembly e-mail system.

ii. Personal e-mails shall not be used to transmit the county assembly's official communication.

iii. E-mail accounts shall have storage quotas which are defined and managed centrally.

iv. E-mails shall not be used to send chain e-mails that generate unnecessary high- volume traffic.

v. Users shall not reply to unsolicited e-mails received.

vi. Automatic forwarding of assembly e-mail to personal external e-mail addresses is prohibited.

vii. Information transmitted by e-mail shall not be defamatory, abusive, involve any form of racial or sexual abuse, contain any material that is detrimental to any party or is outside the specific business interests of the assembly.

viii. The assembly's intranet will be used to communicate all relatively static information (e.g. policies, procedures, briefing documents, reference material and other standing information).

ix. Users shall be required to update their passwords after every (three) 3 months.

x. The assembly mail service shall not be used to broadcast other unofficial information or requests (e.g. information or opinions on political matters, social matters, and personal requests for information)

xi. Email content cleaning will be annually.

z) *Assembly's Website*

The Assembly acknowledges the importance of Website in Communication. The following guidelines shall apply:

i. The Assembly Website shall be managed by the Assembly.

ii. Website content shall be informative and updated.

iii. Web pages shall undergo professional scrutiny and careful preparation before publishing.

iv. The Heads of Department and Sections shall be responsible for the content of published pages and are expected to abide by the highest standards of quality and responsibility.

v. The webmaster shall ensure that the website and pages comply with appropriate policies, branding and standards as well as applicable legal requirements.

vi. All requests for changes on the website shall be subject to the approval of the website editorial committee.

vii. The ICT department shall ensure that the website is always available to the public.

i. *Social Media*

The use of social media is covered by the Assembly Communications Policy. The Assembly's social media activities shall be handled by the Public Communication and Media Relations Section.

ii. *Issuing, Suspension and/or Termination of System Access Privileges*

Process owners shall issue rights to the systems under their usage by approving the Systems Access Request Form for their requesters. The ICT department shall only be charged with the system administration aspect of Information Systems.

User access to Information Systems shall be terminated when:

i. An employee who is a System user exits employment.

ii. An employee is on suspension or temporary detachment from the Assembly.

iii. There is a breach of terms of use on any of the Systems.

iv. The process owner requests for such suspension and/or termination.

Accounts not used for a 90-days period for active systems shall be disabled and deactivated after six-months.

a) Systems Backup

Information Systems shall be backed up regularly to ensure Information Systems, Data and Software can be recovered in case of an incident. The following guidelines shall apply:

i. System administrators shall establish and formally document an appropriate register and schedule for full and incremental backups.

ii. Backup copies shall be retained on a yearly, monthly, weekly and daily basis.

iii. Back-up data must be given a level of physical and environmental protection, consistent with standards applied in the disaster recovery plan.

iv. If data is lost due to logical errors, the database must be recovered up to the nearest possible useful point before the error occurred.

v. After the loss of data, the recovery time will consist of time for: Analysing the error; replacing the required hardware, setting up the operating system and required file systems; restoring the database from the data backups; and performing an instant recovery automatically at system start-up.

vi. Additional backups shall be taken immediately before and after structural change to the database and/or operating system's file so as to ensure

successful restoration in the event that the database or system crash (failure) occurs after the structural change and before scheduled backup.

vii. All systems will be backed up as per the backup schedule maintained by the authorized department.

viii. Periodic restores will be done regularly on the test environment to ensure correctness and integrity of the backup.

The following information shall be documented for all generated data backups: date and time the data backup was carried out (dd/mm/yyyy: hh:mm); the name of the system or short description of the nature of the data; extent and type of data backup (files/directories, incremental/full); backup hardware and software used (computer name, operating system (OS), version number); physical location of the server and the logical path on file-system to the back-up area when fixed media (hard-disks) are used; and data backup and restoration procedures shall be guided by the standard operation procedures (SOP).

CHAPTER FOUR

4.0 ICT SERVICE MANAGEMENT

ICT Service Management is concerned with the management and delivery of ICT resources and core business practices to give end users support for the most desired results in carrying out their day-to-day activities.

The County Assembly of Bungoma shall ensure availability of ICT services as provided for in Operation Level Agreements (OLAs) Service Charter through a centralised management unit responsible for support of all ICT services.

The ICT Department shall develop an Operational Level Agreement (OLA) stipulating its commitment specific to each process owner. This will help to monitor and manage the quality of ICT services in the Assembly. The detailed guidelines are as indicated

1. ICT Help Desk

In an endeavour to minimise disruptions in the provision of ICT Services, the ICT help desk shall ensure that;

i. ICT incidents and service requests are reported through the System and/or e-mail.

ii. All incidences must be put into the helpdesk system and a ticket number issued.

iii. Response to queries is done within the stipulated timeframe outlined in the Service charter and that ICT related issues are resolved promptly.

iv. Service requests are allocated resolution time and an ICT officer to resolve.

v. All the tickets are resolved within stipulated timeframe or escalated to the next level and necessary feedback communicated to the user.

vi. Regular reports from the helpdesk system shall be shared with the Clerk through HOD on a monthly basis.

2. Training

The ICT department shall conduct ICT training and development for ICT users. The following guidelines shall apply:

i. The ICT department in conjunction with Human Resource department shall carry out needs analysis to identify ICT skill gaps.

ii. The ICT department in conjunction with HR and training committee, shall identify and allocate necessary budgets and prepare the training venue(s) and materials for internal training.

iii. All trainings conducted through ICT department shall have a summative evaluation and a training report which shall be sent to the HR and training committee.

iv. Systems users shall receive training for new and existing Information System Software.

3. ICT Service Centre

The ICT department shall establish an ICT support service centre to be run and maintained under service management. The following guidelines shall apply:

i. The Department shall operate a maintenance workshop for ICT equipment.

ii. Faulty or damaged equipment shall be reported or delivered to the service centre using the ICT Asset Movement Form.

iii. A complete backup of Data shall be done on ICT equipment that requires major repairs.

iv. Any faulty equipment shall be diagnosed for identification of fault(s). The identified faults shall be logged and rectified within the stipulated time in accordance with the ICT Service Charter.

v. In a case where a technical officer is unable to repair the equipment, he/ she shall escalate the issue to the immediate supervisor or the contractor responsible for maintenance for a resolution within the stipulated timeframe.

vi. Broken-down ICT equipment shall be declared as damaged if assessed and found to be no longer functional.

vii. Service management shall notify the user once the equipment has been repaired.

viii. ICT equipment shall have a recommended usage lifespan of five (5) years to be replaced subject to availability of funds.

4. Operational Level Agreements (OLA)

The following guidelines shall apply for Operational Level Agreements:

i. The ICT department shall establish and maintain Operational Level Agreements (OLA) with Heads of Department and Sections on ICT services offered.

ii. Annual OLA Reports shall be prepared and submitted to management by the ICT Steering Committee.

iii. OLA monitoring and evaluation shall be carried out by the ICT Steering Committee.

5. Service Level Agreement (SLA)

The Service Level Agreement shall be guided by the following:

i. The ICT department shall establish and maintain Service Level Agreements with third party providers offering ICT services.

ii. The Service Level Agreement shall describe the responsibilities of parties, penalties and specifications outlined in the scope before commencement of ICT project.

iii. The monitoring process and reporting of Service Level Agreement shall be established.

iv. All documentation of ICT projects undertaken shall be kept under safe custody by the Clerk.

v. Information regarding Service Level Agreement for all Systems and Software maintained by Contractors shall form part of the contract and a copy kept by the Clerk.

6. Management Of ICT Service Providers

The Department ICT shall co-ordinate the activities carried out by all ICT Service Providers to ensure services offered meet the business needs of the Assembly. The following guidelines shall apply:

i. The Department shall ensure cordial working relationships are established and sustained with the Service Providers.

ii. A monitoring and reporting mechanism on performance of the Service Providers shall be established as per the Service Level Agreement.

iii. Service providers personnel carrying out works in the Assembly shall be provided with Assembly's Temporary Identification Cards that shall be put on at all times while at the Assembly Premises.

iv. The Temporary Cards shall be surrendered back to the Assembly on completion of the task being undertaken through the office of HR.

v. The Service Providers shall provide all the necessary clothing and tools for their staff in compliance with Occupational Safety and Health Act.

vi. The Service Providers shall provide their staff with dust-coats with their company logo which shall be worn at all times when at the Assembly Premises.

7. ICT Projects Management

In order to ensure only viable projects are implemented, ICT Projects shall be approved by the Board on advice from the ICT Strategic Committee. The ICT steering committee shall monitor the implementation of all major ICT Projects and make recommendations to the Clerk. For the day-to-day running of Complex ICT Projects, the Committee shall establish a Contract Implementation Team (CIT) as per the Procurement laws with the responsibility to monitor and implement the ICT Projects. The ICT department, together with the user Department, shall play a leading role in the management of these Projects with the Head of ICT responsible for:

i. Ensuring that all projects undertaken conform to the Government's ICT Project

Management Procedures.

ii. Preparing and maintaining technical project documentation that include but not limited to project Plans, Schedules, Budget and the risk analysis in consultation with the contractor and Contract Implementation Team.

iii. Ensuring compliance with all internal procedures for managing projects.

iv. Establishing a reporting mechanism to ensure implementation of projects within the specified timelines and budget provisions.

v. All other non-complex ICT Projects shall be carried out by the ICT department.

8. Hardware Maintenance

In order to minimise downtime and ensure continuous functionality of ICT equipment, the ICT department shall conduct regular maintenance of all ICT equipment. The HOD shall ensure that:

i. For specialised equipment, only certified manufacturer’s authorised Agents are

allowed to provide Maintenance Services for ICT equipment in the Assembly.

ii. All ICT Hardware equipment is maintained at an optimal, operational and secure level.

iii. All critical ICT Hardware have running Service Level Agreements.

iv. For traceability and identification, all hardware shall be **bar- coded** and included in the Assembly’s asset register. This shall include any hardware bought for /donated to the Assembly by external agencies.

v. ICT devices are susceptible to theft and unauthorized access, thus, strong security measure to safeguard them shall be provided.

vi. Portable or laptop computers shall not be left unattended in public places, and shall be carried as hand luggage for security.

vii. Portable computing equipment for short term lending shall be stored in secure lockable cabinets.

viii. An updated register of all ICT equipment e.g. LCD projectors loaned out to authorized personnel shall be maintained.

ix. All data storage media shall be stored in secure environments that meet

manufacturer’s specifications for temperature and humidity.

x. Hard copies of systems documentation shall be physically secured in filing cabinets when not in use.

xi. It is the **responsibility** of respective users of any non LAN- connected and official computing equipment (especially laptops/notebooks) to arrange with the ICT support for installation of antivirus software and to perform periodic (at most every fortnight) updates to the antivirus.

xii. All ICT hardware or software will not be taken off-site from Assembly offices, for servicing and /or upgrading without written authority from the Clerk

Printers, Telephone Lines, Fax, Scanners and Copiers

i. Assembly Staff are expected to use the above peripheral devices responsibly. Irresponsible usage of these facilities for personal gain is prohibited, and may lead to denial of the service and/or surcharge.

ii. Where possible, users are required to print on both sides of the paper. ICT support team will give guidance on how various printers are able to print both sides.

iii. Printers will be configured to be shared by many users and placed in secured open offices where possible.

iv. Unofficial calls will be charged on the user.

v. An electronic document scanner shall be used to minimize usage of machines, printers and copiers, saved in suitable formats and emailed to recipients.

B.A.R.S (Biometrics Attendance Register System)

Guidelines for B.A.R.S (Biometrics Attendance Register System)

The following guidelines shall apply

i. The Biometric Attendance Monitoring System shall be maintained as the record of attendance which employees will be required to clock In and Out every time they move in or out of office.

ii. The Biometric Attendance Monitoring System shall be maintained as the record of attendance for MCAs to clock In and Out during Committee meetings and Plenary sessions.

In the exceptional case where an official's fingerprint does not read he/she needs to make manual entry in a register available at HR for employees and

S.A.A for MCAs with In/Out Time & email to info@bungomaassembly.go.ke The in-time considered in such a case will be 5 minutes prior to the email received on info@bungomaassembly.go.ke. That implies that the official needs to mail immediately entering the office. This practice will be allowed at most for 2 days in a month.

For out-time on day the fingerprint is not working for the employee he/she needs to mail on info@bungomaassembly.go.ke prior to their leaving the office along with manual entry in register available at HR for employees and S.A.A for MCAs.

iii. For Employees at other locations, out stations or on any other official duties where biometric attendance system is not available, HONOR system will be considered for monthly attendance, wherein employees need to give declaration for the duties & leave which will be verified by the HR Department.

Honor System is principally based on assumption that the right information has been provided by the employees at out stations. If any information is found to be incorrect later upon verification, then disciplinary action will be initiated against the employee. This disciplinary action could lead up to termination.

iv. Regular office timings are from **8.00am to 05:00pm** with 60 minutes of lunch break on Weekdays.

v. Any Early Out for Lunch or Late In from Lunch will be deducted from working Hours for monthly salary calculations.

vi. Any away from office for official work will require a punch of employee out in biometric machine & clearly mentioned entry of visiting address, purpose, out time, in time & reporting supervisor's name for later approval in register available at HR. Any incorrect information so given by the employee which does not tally with HR will attract disciplinary action which could lead to termination.

vii. If any employee works directly from home based on prior supervisor approval he/she will need to send an e-mail on info@bungomaassembly.go.ke keeping reporting officer in cc, where official In punch will need to be marked in the biometric system.

viii. If any employee is out for personal work he/she will require approval from supervisor & punching for off/ leave in biometric system.

ix. We have no overtime system. If your pending work or supervisor requires any extra work hours no overtime shall be paid. Exceptionally in case of any extraordinary late out, say if beyond 10:00 p.m. in such case supervisor at his/her discretion may allow Late In on the very next day.

    Such confirmation need to be mailed on info@bungomaassembly.go.ke by supervisor. In no case any late out can be adjusted against the any Late In during the month. An employee who works full day (not less than 5 hours) on Sunday/holiday at the request of the supervisor in office or at sites shall be eligible for compensatory off. Any meetings on Sunday/holiday less than 5 hours are not eligible for compensatory off.

x. If an employee requires a Compensatory off, he has to submit the leave approved by his supervisor before proceeding on leave. In case of any emergency, the employee can intimate on info@bungomaassembly.go.ke keeping supervisor in cc.

    The compensatory off application can be submitted later within 2 working days after resuming at work.

xi. No compensatory off will be provided for travelling after working hours or Sundays or Holidays.

ICT Training

Assembly's ICT training needs shall be assessed by the ICT Section and recommendations captured in the Assembly's training plan.

The ICT Officer shall recommend ICT trainings relevant for every section and forward requirements to the Staff Training Committee.

Assembly staff will be trained on emerging technologies as the Assembly may determine from time to time in consultation with ICT department.

4.1.1 DATA AND INFORMATION SECURITY

The County Assembly of Bungoma shall secure its data and information against breaches and threats by preserving its Confidentiality, Integrity and Availability. A vulnerability assessment and penetration testing of all systems and infrastructures shall be undertaken on a bi-annually basis and reports presented to the ICT Steering Committee. The detailed guidelines are indicated.

CHAPTER FIVE

5.0 DATA AND INFORMATION SECURITY

ICT Security policy guidelines are aimed at safeguarding ICT Information Systems, Infrastructure, Information Assets, Computer Networks and Internet against any threats and to ensure confidentiality, integrity and availability of Assembly's ecosystem and data therein. The following guidelines shall apply:

LOGICAL SYSTEMS SECURITY

Users shall be issued with the level of access to ICT Systems required to perform their official duties after making application through the Head of Department.

Adequate systems security shall be put in place to ensure protection and integrity of ICT Systems.

1. There shall be an access control system maintained over all Information Assets according to their classification.
2. No User shall bypass any security control without the approval of the Clerk.
3. All Users of ICT Systems shall be **RESPONSIBLE** for the protection of information resources under their custody.

The Head of ICT Department shall, on behalf of the Clerk:

i. Be responsible for all Information Assets.

ii. Protect the ICT Systems and Services through effective control of security risks.

iii. Establish appropriate controls to limit access to ICT infrastructure, computer equipment, data and information.

iv. A breach of security shall be handled in accordance with the Assembly disciplinary procedures and/or the laws where necessary.

Classification of Information:

Purpose

In order to ensure that the Assembly's information is given the appropriate level or protection, it shall be classified to indicate the need, priorities and expected degree of protection when handling the information. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of security protection or special handling. A security classification system is used to define an appropriate set of security protection levels and to communicate the need for special handling measures to users.

Scope

This standard applies to all employees, temporary contractors and third parties employed by the Assembly and covers all information assets in whichever form they exist (including paper, fax, electronic mail and computer systems).

It applies to all the information that is stored, processed, created, transmitted and/or destroyed in the course of Assembly's business.

Guidelines

The following principles describe the implementation of Information

Classification within the Assembly:

1. The Originator or Information Owner is responsible for setting the

   classification marking of information & media.

2. Classification of Information shall take place at the following levels:

   a) For paper documents, including output from systems, classification shall apply to each individual document;

   b) For cloud-based systems, classification shall be done at the file or dataset level;

   c) For information in a database, the classification shall normally apply to the entire database;

   d) USB's, External Hard Disks, CD's, DVD's and other information carriers shall be classified at the highest category of information carried.

3. Information media shall be marked as follows:

   a) Classification rating, including any handling directives/modifiers, at bottom of every page (paper, front and back, or electronic).

   b) Label on USB's, External Hard Disks, CD's, DVD's, diskettes, tapes etc.

Classification Markings

Classification markings are defined below

PUBLIC
INTERNAL
RESTRICTED
CONFIDENTIAL

PUBLIC

This is information that may circulate freely outside Assembly and, therefore, does not require any special protection. Examples:

i. Published job vacancies.

ii. Assembly's public statements or announcements.

iii. Published promotional flyers.

iv. Advertisements.

v. Final and Signed audited accounts

vi. Salary ranges

vii. Adopted Reports of Committees

INTERNAL

This is information for which unauthorized disclosure, particularly outside Assembly, would be inappropriate and inconvenient; moreover, if this information were to be disclosed to a third party, it could provide a slight reputational disadvantage. This is routine business information, which Assembly simply wishes to keep private. This information typically includes:

i. Internal Assembly Policies and procedures for e.g. User access procedures, Job descriptions, Performance Objectives.

ii. Internal Notices

iii. Training course materials.

iv. Departmental Memo's

v. Assembly Policy Documents

RESTRICTED

This is information intended only for specific employees within Assembly based on their job function/role. It is sensitive, and unauthorized disclosure would normally inflict moderate reputational disadvantage.

This information typically includes:

i. Performance appraisal results.

ii. Detailed network diagrams.

iii. Holders Data

iv. Creditors accounts

v. Claimant data

CONFIDENTIAL

This is highly sensitive information available only to Assembly Top Management and select members with a need to know. Its disclosure to any other employees or to the public would cause severe damage to the interests of Assembly e.g. severe loss of reputation, profit and opportunity.

This information typically includes:

i. Network security configurations.

ii. Planned employee promotions

iii. Board meeting minutes.

iv. Management advisory meeting minutes

v. Disciplinary hearings.

vi. Payroll reports.

vii. Personal Identifiable Information e.g. ID numbers that relates to claimants.

viii. Payment data relating to customers including bank account details.

3.1. Unacceptable Information Systems Usage

The following Activities shall be strictly prohibited without any exceptions:

i. Sharing of employee individual access privileges.

ii. Usage of pirated Software on/in Assembly's Information Systems.

iii. Introduction of any malicious Software on/in Assembly's Information Systems.

iv. Any user action that disrupts or interferes with the normal Assembly's Information Systems usage.

v. Any password cracking, software spying, privilege escalation, unauthorised network port scanning and network reconnaissance, network and/or software penetration.

vi. Installation or use of unauthorised software or information system.

vii. Use of assembly software or information system outside the assembly without approval of an authorised is prohibited.

viii. Duplication of the assembly softwares without approval by authorized officer is prohibited.

3.2. Password Management

The following guidelines shall apply in defining the password strength and lifecycle specifications for all Users:

i. Passwords shall be kept confidential and under no circumstance be shared.

ii. User name accounts or part of the User's full name will not be part of the password.

iii. Passwords shall be composed of the following:

a) A minimum of eight (8) characters.

b) Alpha numeric, special characters, mixed characters' case and text.

c) The last three passwords should not be reused.

d) Note: do not use < or > in your password, as both can cause problems in Web browsers

iv. Default Information Systems and Software Passwords shall be changed on first log in.

v. Passwords must be changed every 90 days.

vi. Password must not be written down.

vii. Passwords must be changed immediately if there is suspicion that the password confidentiality might be compromised and this reported to ICT Department for monitoring.

viii. An in-house developed Information System shall use and support password encryption and user role segregation.

ix. In a case where a System has one administrator, the password escrow procedure shall ensure that an authorised person can access the Administrator's Account in case of an emergency.

x. When temporary access Accounts are required for Internal or External Audit, Software development, Installation or other reasons must be:

a) Authorised.

b) Created with specific expiry date and time.

c) Deactivated and removed from the list of active Users upon expiry of the period.

xi. All non-Assembly users must sign Non-Disclosure Agreement (NDA) before account access is enabled.

xii. Passwords shall not be included in log on scripts or other automated log on processes.

xiii. Password resets shall be requested only by the Owner of the Account through approval from their respective HODs / Sectional heads, except in exceptional cases as may be determined by the ICT Department.

xiv. Violation of the password guidelines may result to disciplinary action and /or legal action.

3.3. Cyber Security

The following guidelines shall apply to Cyber Security:

The Assembly shall have a Computer Incident Response Team (CIRT) whose mandate is to coordinate response and manage Cyber Security Incidents in the Assembly and to collaborate with relevant actors on matters related to Cyber Security.

CIRT shall be the Cyber Security point of contact and is mandated with offering advice on Cyber Security matters in the Assembly and coordinating response to Cyber Security incidents in collaboration with relevant stakeholders as may be approved by the Clerk.

The CIRT shall:

i. Be the risk owner for Cyber Security and will ensure that:

a) The internal ICT Systems are not a source of cyber risk.

b) Data exchange between the Systems complies with all security requirements and best practices.

c) Risk register is maintained.

ii. Ensure the implementation of the Information Security Management System (ISMS) Framework in the Assembly.

iii. Ensure that only authorised users are allowed to access information and data

on the Assembly network.

iv. Provide leadership for the Governance of Cyber Security within the Assembly.

v. Co-ordinate and lead the rollout of periodic cross-cutting security awareness and training to all the employees of the Assembly.

vi. Co-ordinate a vulnerability assessment and penetration testing of all Systems and Infrastructure in the Assembly on quarterly basis.

vii. Ensure that all ICT equipment is installed with the appropriate active malware protection that is continuously updated.

viii. Participate in the activation of the ICT Business Continuity Plan/Disaster Recovery Plan.

3.4. Bring Your Own Device (BYOD)

The Assembly shall allow employees to bring their own devices in strict adherence to the following guidelines:

i. The devices are approved and registered by the ICT department.

ii. The devices must have current Assembly minimum security configurations and software specifications.

iii. Devices must have no sensitive or confidential data, information and Information Systems stored or installed in them.

iv. The Assembly shall have the right to investigate and or audit such devices for any malicious activity, cybercrime or fraud without notification.

v. The device is subject to all Assembly's processes and configurations.

3.5. Business Continuity Plan

The County Assembly of Bungoma shall develop and maintain a business continuity Plan with DRP (Disaster Recovery Plan) specific to ICT which will include critical information systems, ICT Infrastructure and information assets as indicated.

Guidelines for Disaster Recovery Plan

The ICT Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) provide a structured approach for responding to incidents that cause significant disruptions to critical ICT Services in the Assembly.

The following guidelines shall apply:

i. The Assembly shall establish an ICT BCP/DRP as part of the Assembly's Business Continuity.

ii. DR Site shall be established and maintained as per the ICT BCP/DRP.

iii. ICT Department shall ensure that business operations are restored or maintained in the required time in case of any disruption of service.

3.6. Video/Tele Conference Meetings

The following guidelines shall apply during virtual meeting:

ICT shall recommend use of a secure robust System that can be centrally controlled. A System where only invited participants are allowed access shall be used.

The following guidelines shall be followed when attending and convening video/tele conference meetings:

i. Assembly staff shall adhere to all processes during physical meetings as much as practically possible.

ii. Confidentiality – These meetings are official records of the Assembly and confidentiality must be upheld.

iii. The chair must make sure only those supposed to attend by taking a roll-call of the attendees before proceeding.

iv. Preparation of meeting materials and protocols should be observed before presentation of documents including timely circulation and all necessary approvals.

v. Members will go through the documents in good time to provide insightful input.

vi. The secretary of the meeting will prepare writing materials for minutes/record taking in good time before a meeting starts.

vii. Each participant shall ensure their technology works. Ensure availability of a good internet connectivity. Tools will have enough charge to avoid disruption.

viii. Using devices in the following priority; laptop, iPad/tablet and phone will be considered.

ix. Participants will have one device as a backup where possible preferably a tablet or a phone.

x. Participants shall join a video/teleconference meeting before it starts to have time to settle as necessary. This will help address any technological hiccups which will prevent disrupting an ongoing meeting.

xi. Participants must prepare for such meetings professionally. Dress professionally even when dressed casually.

xii. Participants will be aware of the surroundings, making sure the background is professional with similarity to an office setting as much as possible. Preferably plain walls, plain fabric, closed cabinets or similar background. Some conferencing facilities allows you to blur the background helping to address this problem.

xiii. Participants will select a quiet place to avoid both internal and external disruption and noise.

xiv. For a video conference, participants shall turn on camera and remain visible. Adjust the camera angles for the frame to fit appropriately. Camera shall remain on even when a participant leaves their seat.

xv. Participants will make sure there is enough light where they conference from. Have the source of light in front with the darker side being behind. Participants will avoid sitting with the window behind them as the light will make one to be poorly visible.

xvi. Participants will remain seated and present – using attentive body language, avoiding unnecessary leaving meetings too many times which create disruption.

xvii. Participants will avoid fiddling with the Keyboard as Laptops have an inbuilt microphone which captures keystrokes making them disruptive to other members.

xviii. Participants will mute the mic when not talking – This reduces interference from any surrounding noise and makes the contributing person be clearly heard.

xix. Participants will project the voice to make everyone and especially the person taking minutes, record clearly without interrupting the meeting. The recording person will request for a pardon for any clarification.

xx. Food is not allowed in meetings.

xxi. Ear/Head Phones will be used where possible. This reduces possibility of eavesdropping into the meeting.

xxii. Echo will be reduced by having only connecting one device at a time. Connecting two devices at ago in the same location causes feedback causing echo or other irritating sounds.

3.7. Cloud Computing Services

Cloud Computing is a concept that refers to services, applications, and data storage delivered online through powerful file servers interconnected through the internet infrastructure. It allows consumers and businesses to use applications without installation and access their data and information at any computer with internet access. The Assembly's take-up on the use of Cloud Services shall be approved on a case by case in-line with existing government standards, policies and guidelines. The guidelines to be applied shall be as indicated:

Guidelines on Cloud Computing

These guidelines outline best practices and approval processes in relation to the use of cloud computing solutions that the Assembly may decide to use to support data processing, sharing, storage and management.

Cloud computing refers to the delivery of computing services over a third- party proprietary System through Internet. These services involve Infrastructure Development Platforms and Software Applications. The Assembly shall use internal cloud and government cloud where applicable with external cloud services being used with the express authority of the Clerk.

The following shall be considered before considering any cloud computing solutions involving the Assembly Data:

i. Existing Government Policies and set Standards.

ii. The type of Information and Data to be stored, their confidentiality and sensitivity.

iii. The Country where the Service Provider or the Cloud Servers is located in line with the Government Policies.

iv. The available risk mitigation measures and mitigation costs for External, Public and Hybrid Clouds, including encryption of Data, segregation of Data, and appropriate contractual clauses.

v. Whether storage of the Information and Data in question requires the agreement of, or at least consultation with, Staff and/or Third Parties.

vi. Encryption mechanisms.

vii. Physical segregation of the Assembly's records on dedicated Servers.

viii. Use of Cloud Services located in Countries with no intrusive Data Security Laws.

ix. Development of special contractual terms and conditions to ensure the protection of the Assembly's privileges and immunities.

x. A legal contract Non-Disclosure Agreement (NDA).

xi. Have appropriate Service Level Agreements with Vendors

3.8. Electronic Waste (E-WASTE)

All obsolete and unserviceable ICT equipment shall be disposed of in accordance with relevant NEMA E-Waste Regulations and the relevant Public Procurement and Asset Disposal Act, 2015

3.9. Data Management

Retention and disposal of data no longer with special reference to regulatory requirements and business need shall be disposed of as per the County Assembly of Bungoma Records Management Policy.

4.0 Risks

The risks associated with the implementation of this Policy are as indicated.

TYPE OF RISK	**MITIGATION MEASURE**
Poorly managed access to Systems and Information Assets could lead to Users having anonymity or excessive System privileges which could be abused to cause financial and/or reputational damage.	Proper use and authorisation of Systems using System Access Form
E-mail and other electronic communication platforms are not secure by design. The content transmitted could be sensitive in nature and unauthorised accessor negligence in using the Systems could lead to legal issues, reputational or financial damage.	Email and other electronic communication facilities provided by the Assembly are for official business tools and information transmitted via these facilities will be considered business information, owned by the Assembly. Personal emails shall not be used for official communication. Disclaimer at the bottom of emails will be added.
Poorly configured and managed computing Assets could be a vehicle through which unauthorised access to Systems and Information Assets could be obtained.	All Assembly equipment and those being used to transmit Assembly's information (BYOD) shall be configured as per the Assembly Standards
In-appropriate use of internet resources could have a negative impact on infrastructure capacity and availability. It could also expose internal resources when re-used credentials get	Internet must be used as per the internet guidelines herein

compromised on external web platforms; and illegal activity by employees could expose Assembly to legal and reputational risk	
There may be a risk of vulnerabilities or threats (internal and external left unattended, which may be exploited by malicious Users or outside Attackers and may lead to the disruption of Assembly Activities, Sensitive Information Disclosure, Fraud and potential reputational damage.	Regular Systems updates, Patches installation and Systems upgrade must be done as per the Systems guidelines herein.
Unattended vulnerabilities or threats (internal and external may be exploited by malicious Users or outside Attackers an may lead to the disruption of organisational Activities, Sensitiv Information Disclosure, Fraud and potential reputational damage.	All reported/known vulnerabilities must be addressed immediatel and recorded in the Service Desk System for rectification and automati escalation.
Incidents not logged, prioritised, authorised or contained coul lead to a disruption of the Assembly business Activities an damage its Information Assets. This could result in th extended unavailability of key Systems due to failure of addressing incidents	
Unauthorised, poorly tested and /or inadequately documente changes to IT Systems affecting the Assembly's Informatio could cause disruption to production Systems, increase th	All changes to IT Services must follow the Assembly Chang Management process by filling the Change Request forms.

risk of System and Information integrity being compromised o create vulnerabilities in Systems that can be abused by Partie with malicious intent.	Systems must be properly tested in the test environment befor being introduced to the production environment.
A disaster, infrastructure failure or a cyber-attack could rende business critical information un-available. If the busines cannot restore the information from backups, it could lead to breakdown of business processes.	ICT Business Continuity/Disaster Recovery Plan must be update and tested with all relevant backups being regularly done as pe this Policy.
Physical unauthorised access to areas or infrastructure wher sensitive equipment are kept or information is processed, coul create opportunity to disrupt processing change or leak of sensitive Information.	ICT facilities must be designed with risk of data-loss in minc Access to ICT Cabinets and Data Centres must be with an IC Officer accompanying the Third Party who must sign the Dat Centre Rules and Regulations.
Poor selection of outsourcing services could create gaps in th security posture.	All outsourced Services and Locations must have agreement protecting the Assembly's Data with serious legal implications o breach.
Risks may be incorrectly identified and communicated withi the enterprise.	Appropriate risk responses need to be put in place for eacl incident reported.

4.1 Policy Implementation

The County Assembly of Bungoma shall use the existing administrative structures to implement this Policy.

4.2 Monitoring and Evaluation

This Policy shall continuously be monitored and evaluated in line with the existing Monitoring and Evaluation Guidelines of the County Assembly of Bungoma.

4.3 Policy Review

The Policy shall be reviewed from time to time to align it to government policies, legal requirements to keep in tandem with changes in technology, statutory regulations and any emerging issues as the Assembly may deem appropriate.

4.4 Policy Enforcement

Failure to comply with this Policy, standards, guidelines and procedures can result in disciplinary actions as per the HR Manual for employees or termination of contracts for contractors, partners, consultants and other entities. Legal action may also be taken for violations of applicable regulations and laws.

ANNEXURES

ANNEX I: ICT EQUIPMENT ALLOCATION MATRIX

The Assembly shall use the following guideline when issuing computing resources:

DESIGNATION	LAPTOP	DESKTOP	TABLET	PRINTER	CATEGORY
SPEAKER	√	√	√	√	1
CLERK	√	√	√	√	1
DCs	√	√	√	√	1
HODs	√		√	√	1
Deputy	√		√	√	2
OFFICERS I & BELOW		√*		√**	3
SECRETARIES		√		√**	3

Category – Classification of the specification of Laptops and or Desktop Computers

4.2.1. – High End

4.2.2. – Standard

4.2.3. – Basic

√* Issuance of the laptop is subject to written justification that will be based on duties.

√** Shared Printer.

ANNEX II: ICT EQUIPMENT ACKNOWLEDGEMENT FORM

DOCUMENT NO:	CASB/ICT/FORM.1.0	Revision NO.	01	Revision date:	16/01/2023
Title:	ICT EQUIPMENT ACKNOWLEDGEMNT FORM				
Employee Details					
NAME:			PNO:		
DESTINATION					
DEPARTMENT			SELECTION:		
OFFICIAL EMAIL					
SUPERVISORS					
				Tick where applicable	
ICT Equipment's Details				YES	NO
TYPE:			POWER CABLE		
MAKE:			BAG		
MODEL:			MOUSE		
SPECIFICATION:	OTHERS:		KEYBOARD		
SERIAL NO:			ASSET TAG		
COLOUR:			COMMENT(S)		

I acknowledge receiving the above equipment in good physical and working condition from the assembly.im solely responsible for this device until it is returned to assembly ICT Department at the time of my separation from employment or on request from assembly through the clerk. I will strictly use the equipment for official purpose only. By signing this document, am accepting and agreeing to all assembly's usage and policies.					
Employee Signature			Date:		
Authorized issuing ICT officer					
Name :		Sign:		Date:	

ANNEX III: ICT EQUIPMENT MOVEMENT FORM

COUNTY ASSEMBLY OF BUNGOMA

Document No.:	CASB/ICT/ FORM.2. 0	Revision No:	0.1	Revision Date:	16/01/2023
TITLE:	**ICT EQUIPMENT MOVEMENT FORM**				
Employee Details					
NAME:				PNO:	
DESIGNATION:					
DEPARTMENT:				SECTION:	
OFFICIAL EMAIL:				SUPERVISOR:	
MOVEMENTDETAILS					
FROM:		TO:			
REASON:					

ITEM	**MAKE/MODEL**	**SERIAL NO.**	**ASSET TAG NO.**	**QTY**

Employee Signature:							Date:	
Authorised issuing ICT Officer								
Name:			Sign:				Date:	

ANNEX IV: ICT SYSTEM ACCESS REQUEST FORM

COUNTY ASSEMBLY OF BUNGOMA						
Document No:	CASB/ICT/FORM.3.0	Revision No:	0.1	Revision date	16/01/2023	
Title:	**ICT SYSTEM ACCESS REQUEST FORM**					
Employee Details						
REQUEST NAME:						
DEPARTMENT NAME:						
OFFICIAL EMAIL:						
SIGNATURE			Date			
System Requested for Access (tick as appropriate):						

NO	**SYSTEM**	**Tick**	**CREATED BY**	**SIGN**
1	Active Directory			
2	Customer Management System			
3	Electronic Document Management System			
4	Email			
5	Help desk			
6	HRMIS			

7	BAR			
8	Website			
9	Intranet			
10	Internet			
11	Asset Management System			

Request Type: New user Change/Modify user Deactivate user HOD Approval:

Systems Approval (How many) [_] specify the system (No 1,4,) ....

Approved by P No .... NAME: ....

Designation: ....

Signature: .... Date:...

Department/section:... ....

<u>ICT Approval:</u>

Approved by P No: ....Name: ....

Designation: ....

Signature: .... Date:.........................

Specify the systems (e.g.,a,b,c etc ....

ANNEX V: ICT SYSTEM CHANGE REQUEST FORM

COUNTY ASSEMBLY OF BUNGOMA					
Document No.:	CASB/ICT /FORM.4. 0	Revision No:	0.1	Revision Date:	16/01/2023
Title	ICT SYSTEM CHANGE REQUEST FORM				
Employee Details					
REQUESTER NAME:		PNO:			
DEPARTMENT:		SECTION:			
OFFICIAL E-MAIL:		DESIGNATION:			
SIGNATURE:		DATE:			
Change Request					
Change Description/Change Request Filename:					
System		Needed by			
Description of the change:					

Reason for the change:							
Requestor Sign off:							
Process owner Approval:							
Change impact Evaluation							
Change Type	Applicatio n		Database				
	Hardware		Procedures				
	Network		security				
	Operating System/ Utilities		Schedule Outage				
Change Priority	Urgent/ High/ Medium/ Low		Change impact	Minor / Medi u m/ Major			
Environment(s) Impacted:							
Resource requirement:(personal,HW,SW)							
Test Plan description:							
Rollback description:							
Change approval or Rejection							
Change Request Status	Accepted		Rejected				
Comments:							

Change scheduled For date):			
Implementation assigned to:			
Clerk Sign off:			
Change Implementation			
Staging test results:			
Implementation test results:			
Date of implementation			
Implementer Sign Off		Date	

ANNEX VI: ICT LOST-DAMAGED EQUIPMENT REPOTING FORM

COUNTY ASSEMBLY OF BUNGOMA

ICT LOST-DAMAGED EQUIPMENT REPORTING FORM

Document No:	**CASB/ICT/FO RM.5.0**	**Revision No:**	**1.0**	**Revision Date:**	16/01/2023
Employee details					
REPORTER'S NAME:			PNO:		
Department:			SECTION:		
OFFICIAL E-MAIL:			DESIGNAT ION:		
SIGNATURE			DATE:		
Type of equipment:		Equipment status (must check one)	Lost	Damaged	Stolen
Incident Date:			Needs replacement (check one)	YES	NO
If stolen/lost,Date reported to					

police:					
If stolen/lost Police Report reference no:					
Police Station reported:					
Description of incident(write briefly what happened to the equipment)					
Equipment Information-check with ICT information					
Type/Make/Model:			Serial Number:		
Repair Cost Estimate			Approximate Equipment Cost:		
Equipment specification details:			Signature		
Designation	Name			Date	
ADD SERVICE MGT:					

All stolen and lost equipment must be reported to the police. Submit this form to ICT after filing a police report.

Copy to send to CLERK and Supply Chain Management Services.

ANNEXURES VII

Classification of information

Label	Description	Encryption	Labeling	Reproduction	Disclosure	Discussion	Dispatch
Public	This classification applies to the assets containing the information which has been explicitly approved by the management for release to the public	Not required for information at rest or in motion	N/A	N/A	N/A	N/A	N/A
internal	This classification applies to the assets	Information in motion Not required	Appropriate marking to be added in on the	N/A	Organization wide	In Assembly's spaces and in selected	Sealed envelop, electronically to the named

	containing the information of Assembly which is meant for use by employees	information at rest; Encryption Desirable	bottom of the item (each page)			third party spaces	group within the assembly
Restricted	This is a highly sensitive information available to Assembly Top Management whose disclosure to any other employees or to the public would cause severe damage to he interests of	Information in motion; encryption Desirable. information at rest Encryption Mandatory	Appropriate marking to be added in on the bottom of the item (each page)	Only within owner’s permission	Team need know basis	In assembly’s spaces with defined set of participants	To be handed to named address, in in person. Mark/label email header and on sent named recipients.

	Assembly e.g., sever loss of reputation, opportunity						
Confidential	This classification applies to the assets containing the information of Assembly which if disclosed (either within or outside the Assembly to unauthorized individuals, altered misused, or destroyed will cause	Information in motion; encryption mandatory. Information at rest; encryption Mandatory	Appropriate marking to be added in the bottom of the item (each page)	Only by or on behalf of owner	Individual need to know Basis	In Assembly's spaces with defined group of participants space is secured	To be handed to named address, person. Encrypted transfer and email sent on to named receient

	damage to Assembly’s stakeholders, partners and employees. This information, if not adequately protected, may result in non-compliance with applicable laws and regulations. Access to this information require approval from the owner of the information						

	and shall be given on a need-to-know basis						

REFERENCES

1. The National ICT Policy 2019
2. The ICT Standards 2016 (first edition)
3. The Constitution of Kenya.
4. County Assembly of Bungoma Strategic Plan 2022-2031
5. Kenya Information and Communication Act (2012).
6. Access to Information Act (2016).
7. National ICT Policy (2016).
8. The National ICT Guidelines (2020).
9. National E-waste Policy (2018).
10. Public Procurement and Asset Disposal Act (2015).
11. Public Procurement and Disposal Regulations (2020).
12. Computer Misuse and Cybercrimes Act (2018).
13. Data Protection Act (2019).
14. Occupational Safety and Health Act (2007).
15. Government ICT Standards ICTA-2019.

COUNTY GOVERNMENTOF
BUNGOMA

CONTACTS

P.O. BOX 1886 – 50200 Bungoma

info@bungomaassembly.go.ke

0208000663/0202651905

www.bungomaassembly.go.ke

Bungoma County Assembly

@AssemblyBungoma