REPUBLIC OF KENYA

MINISTRY OF FOREIGN AND DIASPORA AFFAIRS
STATE DEPARTMENT FOR FOREIGN AFFAIRS

INFORMATION COMMUNICATION & TECHNOLOGY POLICY

JUNE 2024

TABLES OF CONTENTS

FOREWORD

The Ministry of Foreign and Diaspora Affairs has prioritized use of Information, Communication and Technology (ICT) to achieve its mandate of promoting Kenya's interest and image in line with the Constitution of Kenya, 2010 and Kenya Vision 2030. In a globally competitive world where countries are continuously competing for the same opportunities, people's changing needs and evolving global trends and technological advancement are essential for Growth and transformation.

As the world becomes increasingly interconnected through digital means, the role of ICT has emerged as a cornerstone of global progress and development. It is with great pleasure that I introduce the State Department for Foreign Affair's ICT Policy, which stands as a testament to our commitment to harnessing the power of technology for the betterment of our Nation.

At the heart of our policy lies a vision of leveraging ICT to empower our citizens, bridge societal divides, and create opportunities for all. By investing in infrastructure, promoting digital literacy, and fostering a vibrant ecosystem for innovation and entrepreneurship, we aim to unlock the full potential of ICT to drive sustainable development and improve the quality of life for our people.

Furthermore, in an increasingly interconnected world, cybersecurity and data privacy have become paramount concerns. Our policy emphasizes the importance of building robust cybersecurity frameworks and safeguarding the privacy and security of our citizens' data, ensuring that they can harness the benefits of technology with confidence and peace of mind.

Finally, I commend the State Department for its dedication and vision in crafting this policy, which represents a significant step forward in our journey towards a more connected, inclusive, and prosperous future. Together, let us embrace the opportunities of the digital age and work towards building a brighter tomorrow for generations to come.

Hon. Dr. Musalia Mudavadi, E.G.H
Prime Cabinet Secretary and Cabinet
Secretary for Foreign and Diaspora Affairs

PREFACE AND ACKNOWLEDGEMENTS

The Government of Kenya has underscored universal access to Information, Communication Technologies (ICTs) as a major driver of the Kenya Vision 2030 which is Kenya's economic blueprint that is aimed at transforming Kenya into a middle-income country. Further, the Bottom-up Economic Transformation Agenda (BETA) has been designed to address the current challenges facing the country's economy, stimulate economic recovery and bolster resilience. Digital Superhighway and Creative Industry is one of the five pillars of this Transformation Agenda.

In this regard, the State Department recognizes the critical role of ICTs as an enabler of Service delivery and a central pillar to the delivery of its mandate. It has been undertaking various initiatives geared towards automating its processes with a view to enhancing operational efficiency and effectiveness in service delivery. In addition, the State Department has deployed a number of systems developed by the Government to provide e-services. Some of these systems include: Integrated Protocol Management Information System (IPMIS), Integrated Finance Management Information System (IFMIS), Document Authentication System, Performance Management System (PMS), Government Human Resource Information System (GHRIS) and Treaties Repository Portal.

As our nation progresses in the digital age, the policies formulated by the State Department aim to harness the potential of technology to foster innovation, economic growth, and societal development. Your acknowledgment underscores the importance of these efforts in the broader context of our country's diplomatic relations and global engagement. We remain committed to collaborating closely with the State Department of ICT to ensure that our policies align with the national interest and contribute positively to our international standing. Your continued support and guidance in this regard are invaluable as we navigate the complexities of the modern global landscape.

This policy was prepared through a participatory and collaborative approach involving the State Department's Directorates, Kenya Diplomatic Missions abroad and a wide spectrum of State Department's stakeholders and partners, in line with government policies, ICT Authority standards and legal and regulatory frameworks.

I wish to thank each of them individually and collectively for their invaluable contribution towards preparation of this Policy. The Policy will be reviewed from time to time to respond to the emerging national and global technological dynamics.

Dr. A. Korir SingOei
Principal Secretary
State Department for Foreign Affairs

ACRONYMS / ABBREVIATIONS

DPSM- Directorate of Public Service Management

GDP- Gross Domestic Product

GHRIS - Government Human Resource Information System

GOK - Government of Kenya

HR - Human Resource

ICT- Information Communication and Technology

ICTA - Information Communication and Technology Authority

IFMIS - Integrated Finance Management Information System

IPMIS - Integrated Protocol Management Information System

IPPD- Integrated Payroll and Personnel Database

KRA - Kenya Revenue Authority

LAN - Local-Area Network

M&E - Monitoring and Evaluation

MFDA- Ministry of Foreign and Diaspora Affairs

MTEF - Medium Term Expenditure Framework

NEMA - National Environmental Management Authority

NTSA - National Transport and Safety Authority

PFM - Public Financial Management

PMS - Performance Management System

SLA - Service Level Agreement

SWOT - Strengths, Weaknesses, Opportunities, and Threats

UPS - Uninterruptible Power Supply

USB - Universal Serial Bus

VOIP -Voice Over Internet Protocol

VPN - Virtual Private Network

WAN - Wide-Area Network

GDPR - General Data Protection Regulation.

EXECUTIVE SUMMARY

Information Communication Technology has become the backbone of day to day operations in all organizations. Governments all over the world have become increasingly dependent on ICT to drive development as well as offer efficient and effective services to their citizenry. Kenya is no exception. ICT has been placed at the center of the country's economic, social and political development as espoused in Kenya's Vision 2030, BETA and the National Digital Master Plan 2022.

The formulation and development of this Policy is guided by the Kenya Vision 2030, the National Digital Master Plan 2022, National ICT Policy 2019, National Cyber Security Strategy and various ICT related legislations and standards. The State Department has embraced digital revolution by making substantial investment in ICT resources and infrastructure in order to facilitate achievement of its mandate. The adoption of ICT has enabled the State Department to deliver efficient services such as processing of payments using the IFMIS system, managing staff payroll using GHRIS, Communications through emails and use of social media platforms, increasing the State Department's profile and visibility through use of website and reporting performance using the PMS.

While the State Department developed and implemented a Ministerial ICT Strategy, the absence of clear policy guidelines on ICT has not only adversely hampered service delivery but also exposed the State Department to ICT related risks. To address these challenges, this Policy has been developed with the overall aim of positioning the State Department to effectively utilize the opportunities of digitization to enhance effective and efficient delivery of information and services to its national and international populaces.

The specific objectives of the Policy are to: provide guidelines for effective deployment, management and utilization of ICT resources in the State Department; enhance service delivery by promoting use of e-platforms in provision of State Department services; provide guidelines for ensuring the security of State Department information, ICT equipment and systems; provide a framework for effective management of the acquisition, installation, usage, maintenance and disposal of ICT equipment; and assist the State Department to comply with National and International policies, legal, regulatory and contractual requirements and obligations on ICT deployment and usage.

The Policy further lays a solid foundation for prioritization and effective deployment and management of ICT resources as well as the basis for future resource allocation, both at the State Department headquarters and its Diplomatic Missions.

The successful implementation of this Policy will require full involvement, effort and commitment of the State Department top management, users and stakeholders. This will be critical for the State Department to realize the aspirations of this Policy. In this regard, the State Department will sensitize all staff on the Policy to ensure acceptance and hence build a critical mass for its successful implementation. An annual Monitoring and Evaluation (M&E) will also be undertaken to measure the successes and identify any shortcomings, as well as to determine the level of compliance with the existing policy, legal and regulatory frameworks. The M&E will provide useful feedback on the basis of which informed and evidence-based management decisions will be made.

The Policy will be reviewed from time to time to respond to the emerging national and global technological trends as well as State Department's needs in the use and management of ICT.

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

The State Department has embraced the digital revolution by making substantial investment in ICT resources and infrastructure in order to facilitate achievement of its mandate. The State Department is utilizing shared specialized systems such as IFMIS for procuring goods and services and making payments, Integrated Payroll and Personnel Database (IPPD) for managing payroll, internal and external communication through emails and social media platform, PMS for managing performance contracting as well as IPMIS and Document Authentication System. The use of website has also enhanced State Department's profile and visibility.

The development and implementation of an ICT Policy in the State Department for Foreign Affairs arises from a range of challenges. These include; increasing cyber threats that endanger sensitive data and systems, the need for compliance with legal and regulatory requirements, and the complexities of managing diverse and rapidly evolving technologies. Additionally, the State Department faces difficulties in ensuring consistent and secure use of ICT resources among staff, leading to potential inefficiencies and risks. The growing demand for remote work and digital collaboration tools also introduces new security and operational challenges. Furthermore, there is often a lack of awareness and training among staff regarding best practices for ICT usage which can result in misuse and vulnerabilities. These challenges necessitate a comprehensive ICT Policy to safeguard the State Department, optimize resource utilization, ensure regulatory compliance, and support strategic goals.

1.2 SCOPE AND APPLICABILITY

This policy is applicable to all State Department staff, at the Headquarters and its Missions, its stakeholders, all users of ICT equipment owned or leased by the State Department as well as equipment connected to State Department's ICT related infrastructure. The Policy also applies to all State Department's' ICT related resources and services.

1.3 RATIONALE AND POLICY OBJECTIVES

1.3.1 Rationale.

The Government of Kenya recognizes the fundamental importance of ICT to stimulate national development, in particular, modernization and globalization of the economy, and creating conditions for full participation by all sections of the Kenyan population. Contemporary public service calls for extended outreach and accountability in a multi-stakeholder global arena. In this regard, all Ministries, Department and Agencies (MDAs) are required to develop sector specific policies to leverage on new technologies and address ICT gaps to improve service delivery and increase productivity.

The State Department has increasingly been investing in building its ICT capacity to facilitate its internal business operations so as to attain its strategic goals. Consequently, ICT uptake in the State Department has significantly improved and most functions in the State Department are automated. However, the management of ICTs in the State Department has been ad-hoc with no clearly documented procedures and guidelines. The growing reliance on ICT also makes the State Department vulnerable to ICT related risks. The State Department, therefore, needs to develop and operationalize a comprehensive ICT Policy to guide ICT adoption and to streamline its usage.

This Policy therefore, provides a framework for managing the ICT infrastructure and related user risks in the State Department headquarters and the Missions. It aims to address the challenges being experienced in the State Department by facilitating standardization in the application of ICT procedures and practices, from acquisition to maintenance and disposal. The Policy lays a strong foundation for development of the State Department's priorities and strategic direction in ICT, as well as the basis for resource allocation. Meaningful and well-planned use of ICT is expected to enhance and strengthen State Department's diplomatic engagement and service delivery and help it cope with the emerging national and global challenges in delivery of its mandate within the context of the Kenya Vision 2030, National ICT Policy 2019, Kenya National Digital Master Plan and Kenya Digital Economy Blueprint.

1.3.2 Policy Objectives

The policy seeks to position the State Department to leverage digitization opportunities, enhancing the effective and efficient delivery of information and services to both national and international audiences. The specific objectives are to:

I. Provide guidelines for effective deployment, management and utilization of ICT resources in the State Department.

II. Enhance Service delivery by promoting use of e-platforms in provision of State Department services.

III. Provide guidelines for ensuring the security of State Department information, ICT equipment and systems.

IV. Provide a framework for effective management of the acquisition, installation, usage, maintenance and disposal of ICT infrastructure.

V. Assist the State Department to comply National and International policy, legal, regulatory and contractual requirements and obligations on ICT deployment and usage.

VI. Provide a strategic framework that aligns technology initiatives with the State Department's goals and objectives to streamline planning and implementation of ICT projects.

VII. Provide guidelines and procedures for technology use to promote transparency and accountability. This helps in monitoring and evaluating the performance of ICT initiatives and ensures that resources are used responsibly.

1.4 MANDATE OF THE STATE DEPARTMENT

The mandate of the State Department for Foreign Affairs as drawn from the Executive Order No. 2 of 2023 is to lead in the execution of the nation's Foreign Policy and advise the Presidency on regional, continental and global affairs, with the following functions and responsibilities: -

1. Management of Kenya's Foreign Policy;
2. Projection, Promotion and Protection of Kenya's Interest and Image globally;
3. Management of Kenya's Missions, Embassies and High Commissions Abroad;
4. Co-ordinating Regional Peace Initiatives;
5. Ratifications/Accession to, Depository and Custodian of all International Treaties, Agreements and Conventions where Kenya is a Party;
6. Co-ordinations of Matters Relating to IGAD and Association of Regional Cooperation (ARC);
7. Liaising and Co-ordinating with World Trade Bodies and UN Agencies;
8. Promotion of Nairobi as a Hub for Multilateral Diplomacy;
9. Lobbying for Kenya Candidature in the International Governance System;
10. Liaison with the Ministry of Labour in the implementation of the Labour

Migration Policy;

11. Through Kenya's Missions abroad, support the State Department for Diaspora Affairs in harnessing Kenya's Diaspora for national development;
12. Negotiation and Conclusion of Headquarters and Host Country Agreements with International Organizations and Agencies;
13. Liaison with International and Regional Organizations;
14. Liaison with Foreign Missions in Kenya;
15. Administration of Diplomatic Privileges and Immunities;
16. Co-ordination of State and Official Visits;
17. Protocol and State Courtesy;
18. Provision of Consular Services;
19. Management of Joint Commissions with other Countries;
20. Management of Bilateral and Multilateral Relations; and
21. Official Communications on Global Foreign Relations.

1.5 METHODOLOGY

This Policy was developed by a committee in collaboration with a representative from the Ministry of Information, Communication and Technology and consultants from Sentinel Africa Ltd. It was then shared with State Department staff drawn from its Directorates, Departments, Divisions and Missions for feedback and input. Their views were instrumental in fine tuning the Policy as well as aligning it with the State Department's Strategic Plan.

The Policy was informed by key policy documents namely; Kenya Constitution 2010, Kenya Vision 2030, the National Digital Master Plan 2022, the National Cyber Security Policy and Information Communication and Technology Authority (ICTA) Standards on Information Security and international ICT standards among others.

CHAPTER 2

SITUATIONAL ANALYSIS

Globally, many Governments have embraced technology in provision of services to its citizens. Kenya like other countries established an e-government strategy in 2008 that foresaw the creation of ICT Divisions across Ministries with the mandate of spearheading Government's ICT initiatives.

The State Department for Foreign Affairs, with a diplomatic footprint spanning five continents, recognizes the critical role of ICT in fulfilling its core mandate. It has embraced ICT as a key driver and an enabler in provision of e-services, promotion of the State Department's digital profile and visibility and facilitating communication with its stakeholders nationally and globally.

The State Department has developed and implemented several applications such as the IPMIS system, PMS, Treaties Repository Portal, and Document Authentication System, among other support systems in order to enhance its operations. IP telephony has also been deployed in one Mission with plans to extend it to other missions to improve connectivity, strengthen secure communication between missions and headquarters as well as to reduce costs. Following a feasibility study conducted in some pilot Missions, the State Department in collaboration with National Treasury has completed phase one of IFMIS rollout in the Missions. The main objective of linking missions to IFMIS is to promote financial governance and facilitate real-time financial reporting in accordance with the PFM Act, 2012.

CHAPTER 3

POLICY GUIDELINES

3.1 INTRODUCTION

The Government of Kenya has prepared policies, strategies and standards to guide MDAs in adopting ICT to improve services delivery. MDAs are required to domesticate these national and international frameworks to suit their needs while at the same time contributing to the national ICT theme of propelling Kenya into a knowledge-based economy.

These Policy guidelines have been developed to respond to the national aspirations and to guide the State Department in the adoption, deployment and management of its ICT resources more efficiently, effectively and in a transparent and accountable manner. The guidelines will be applied alongside the Ministerial ICT Strategy developed in 2015.

3.2 POLICY GUIDELINES

3.2.1 Software

The State Department has acquired various software. These include: programmes, codes, operating systems, applications, off-the-shelf packages, databases, data and files among others. The following guidelines will be adhered to in the management of the State Department's software:

- All software in use will remain the property of the State Department.
- All software will have genuine licenses and shall be installed by the ICT division or in case of Missions abroad by an authorized officer designated by Head of Mission.
- Unauthorized software is deemed to be illegal and shall not be installed in the State Department's ICT equipment. Any user who installs unauthorized software will be subject to disciplinary action.

- Copying and/or duplicating software is prohibited. Where this is permitted within the software license agreement, it will be the responsibility of ICT or a designated officer to carry out the duplication/copying. This will be carried out in conformity to copyright laws and software licensing agreements.

3.2.2 Computer Hardware

These guidelines will help the State Department in planning for and maintaining computer hardware. Computer hardware includes desktops, laptops, printers, digital cameras, projectors, UPS, routers, switches, Modems and any other physical component of the ICT installation.

- The State Department will facilitate members of staff with appropriate ICT equipment to effectively perform their duties. An inventory of the same shall be kept under the custody of Supply Chain Management Division in collaboration with ICT Division.

- Users shall be accountable for all ICT equipment issued to them and shall surrender the them to the immediate supervisor for clearance in line with prevailing procedures before exiting the State Department on transfer, retirement or otherwise. In case of damage or loss of an equipment the officer will be held liable.

- All servers other than for backing up and disaster recovery shall be located in a central server room. The ICT division or incase of the Missions an officer designated by the Head of Mission shall take responsibility for administration and management of the server(s) and the server room.

3.2.3 Internet usage and management

The State Department and its Missions abroad provide Internet Service allowing access by staff. Currently, the State Department accesses its internet through an ISP controlled and managed by State Department of ICT. The State Department is however in the process of securing a redundant ISP which will serve as a backup in case of internet failure. The Kenya Missions have independent ISP's. The guidelines below enumerate access rights, usage of internet and conduct of users of internet both at State Department headquarter and Missions abroad.

- Use of Internet for illegal or unlawful purposes is prohibited and attracts disciplinary action. Instances of illegal/ unlawful use includes:- copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling and computer tampering (e.g. spreading computer viruses);

- Users should limit their personal use of the Internet and apply prudence especially during working hours. The State Department will not allow use of social media for personal business during official working hours.

- Users are required to take necessary precautions to prevent unauthorized access to Internet services.

3.2.4 Remote Access

- All Remote access users shall be strictly controlled, and all account activity shall be continuously monitored to prevent abuse or breach of security;
- Users who may be granted remote access privileges should constantly be aware that remote connections between their location and the State Department are literal extensions of the State Department network, which can provide a potential path to the State Department's most sensitive information;
- Remote users shall take every reasonable measure to protect State Department's assets or information that they are allowed to access;
- The State Department reserves the right to disable any remote access account, with or without prior notice to affected user, if abuse is suspected.

3.2.5 Online Meetings

- Staff shall register and join virtual meetings using their official names. Prior communication to the ICT division through a memo shall be used to request for virtual meetings recording.
- Staff shall be expected to adhere to virtual meetings etiquettes

3.2.6 E-mail services

The State Department has created official email accounts for use at Directorate/Departmental/Mission and individual levels. Currently, State Department emails are hosted at ICTA. A number of Missions have contracted mail services which makes it a duplication of effort since the State Department has a working mail system. This does not reflect a cooperate image of the State Department and is discouraged. It's important that all official communication is through the MFA email system.

Access to e-mail is a privilege and certain responsibilities accompany that privilege; users of e- mail are expected to be ethical and responsible in their use. This precludes the sending of mails that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, nationality, disability or religious beliefs. The following will guide the management of official email account: -

- Messages composed, sent or received on the electronic mail system are and remain the property of the State Department, regardless of purpose or content.
- The use of the electronic mail system is reserved solely for transacting official State Department matters. The electronic mail system shall not be used to create any offensive or disruptive messages. Messages that are derogatory include, obscene, pornographic, defamatory, harassing, threatening, contain racial or inappropriate slurs. Contravent ion of this will lead to appropriate disciplinary action.
- Officers will not be allowed to use personal email accounts to transact official business.
- The electronic mail system shall not be used to contravene or violate copyrights or other proprietary rights by distributing unauthorized copies of materials owned by others, nor shall it be used to distribute confidential or proprietary State Department's materials without proper authorization.
- The electronic messaging system shall be monitored to ensure compliance and adherence to guidelines set out in this policy. All traffic originating or terminating on MFA's network is logged and random checks of these logs are conducted periodically for administration purposes.

  Upon termination, transfer or separation from the State Department, the email account and other associated system accounts of the staff in question shall be deactivated.

3.2.7 State Department and Missions Website

The State Department in collaboration with ICTA will develop a global website template which will host Missions websites sub-domains. The global website will provide a one stop shop for accessing the State Department and Missions' information. These mission's website sub-domains will be standardized to conform to the ICTA standards and State Department corporate branding while at the same time enhancing its look and feel. Once the global website is fully operationalized, Missions operating independent websites will be required to pull them down and migrate to the global website. The following guidelines will be used to manage the website and any sub-domains: -

- The Heads of Department and Mission will be responsible for ensuring that materials related to their respective Departments and Mission are accurate and meet the standards which will be issued by ICTA;
- Public Affairs and Communication Division shall be responsible for updating the website in consultation with ICT Unit. Heads of Mission are expected to designate an officer who will regularly update their sub-domains in the global website

3.2.8 Backup

Protection of valuable information is critical. Data including but not limited to word documents, spreadsheets, databases, presentations, and certain e-mail messages must be backed up. However, the State Department has not yet implemented active directory for daily users' backup. Furthermore, the State Department's email system and website are currently hosted and backed up at ICTA.

The State Department will implement a system to facilitate daily backup. Back-ups will be performed on key data and this will be reviewed by the ICT Unit from time to time to ensure that the State Department is not exposed to any risk.

3.2.9 E-Communication

Adoption of Social networks such as Twitter, Facebook, WhatsApp and YouTube have enhanced Government service delivery, information sharing and openness. Kenyan public and private sector are using ICT capabilities to efficiently deliver services, conduct business transactions and share information across organizational, social, and geographic boundaries. The Government of Kenya has widely deployed use of E-communication in line with Constitution of Kenya, 2010, Kenya's Vision 2030 and the National Digital Master Plan 2022.

The State Department has taken cognizance of this development and is using social media tools to complement existing channels of communication to enhance service delivery and share information with its internal and external stakeholders. The following guidelines will apply to ensure proper use and management of social media platforms: -

- Official information posted to the social networks shall have the express authority of State Department spokespersons: The Cabinet Secretary, the Principal Secretary, Director Generals and Heads of Directorates or the Heads of Mission.
- The State Department official accounts on twitter, Facebook and YouTube are designated and managed by Public Affairs and Communication Division or in the case of Missions an officer designated by the Head of Mission.
- Messenger Apps such as WhatsApp and telegrams among others are admissible for internal staff communication.
- The State Department will operate an intranet computing for internal communication and information sharing.
- Restricted, Secret and confidential information shall not be posted in the social media platforms.

3.2.10 Acquisition, Maintenance, Replacement and Disposal

3.2.10.1 Hardware and software acquisition and inventory

A warranty of acquisition for all ICT Hardware and Software shall be obtained with the service providers as the first step of acquisition guided by both the ICT Standards and Public Procurement and Asset Disposal Act, 2015. A Service Level Agreement (SLAs) will always be signed for software acquisition.

Supply Chain Management Unit in collaboration with ICT Unit will keep a comprehensive inventory of State Department's ICT needs to guide acquisition, maintenance, replacement and disposal of ICT equipment. The inventory will be updated twice, at the beginning and end of every financial year. The ICT hardware comprise: Desktops, printers, projectors, laptops, modems, networks and any other component of ICT installations and accessories.

3.2.10.2 Software Acquisition

All software acquired by the State Department and Kenyan Missions will have documentation manuals that bear legitimate contract licenses and not third parties licenses. Delivery and guaranteed functionality of acquired software will be the responsibility of the supplier as stipulated by the manufacturer's warranty. The Head of the ICT Unit or in case of Missions abroad a designated officer will be responsible for ensuring that the guidelines for software acquisition are adhered to.

3.2.10.3 Systems Acquisition

The State Department's Supply Chain Management in consultation with the ICT Unit and Legal Affairs and Host Country Division and the systems developer will prepare a contract/agreement clearly stipulating the State Department's and the developer's responsibilities including a warranty period in which the developer will do maintenance of the system.

3.2.10.4 Repairs and Maintenance

- The State Department will prepare a maintenance schedule for all its ICT equipment and systems.

- Maintenance/repair of ICT equipment and systems will be carried out as per the maintenance schedule.

- Repair work of any ICT equipment will be carried out within the State Department. Where repairs are to be carried out of the State Department premise, the Head of ICT in consultation with the Supply Chain Management Unit will be expected to grant written authorization.

- Maintenance or repair by a service provider will be carried out under close supervision of ICT Unit.

3.2.10.5 Replacement and Disposal of ICT equipment

- The State Department shall keep a comprehensive inventory of all ICT equipment. The ICT Unit will prepare and update on a regular basis the inventory to facilitate planning.

- The State Department will annually budget for replacement of ICT equipment within the MTEF budget process.

- The State Department will dispose any obsolete ICT equipment in line with the Public Procurement and Asset Disposal Act, 2015 and National Environmental Management Authority (NEMA) guidelines on e-waste.

3.2.10.6 Software disposal

- Once a software becomes obsolete, data will be moved to another system, archived, discarded or destroyed in accordance with the State Department's data retention procedures.

- Data contained in equipment earmarked for disposal shall be permanently erased for security of the data

3.2.11 User support

The State Department has a help desk which supports users through provision of immediate services not requiring external contractor, such as diagnostic and configuring of ICT components (hardware and software). The Missions will be mapped in regions and ICT officers will be allocated Missions to support from headquarters and where need be by going to the region.

The Missions shall ensure that a person contracted to support is known and can be trusted to handle Mission information. Where a system is handling sensitive information, an ICT officer supporting that region will be invited to assist to address and provide the necessary support.

CHAPTER 4

ICT SECURITY GUIDELINES AND RISK MANAGEMENT

4.1 INTRODUCTION

Information and data are important State Department assets. Therefore, like any other physical assets, ICT equipment and systems must be protected from security threats such as disclosure, hacking, cyber-attacks, unauthorized access, loss, corruption and interference. The State Department has developed this policy to ensure an adequate level of security is attained and the best security practices are adopted in the deployment and management of State Department's ICT resources.

These guidelines have been prepared in conformity with Government policies and standards such as Kenya National Cyber Security Policy and ICTA standards on Information security as well as International Information Security Standards.

4.2 PHYSICAL AND LOGICAL SECURITY GUIDELINES

There are two categories of IT Security, namely; Physical Security and Logical Security. The State Department will apply the following guidelines to enhance physical security of its ICT resources.

4.2.1 Physical Security

4.2.1.1 Server room

The following measures shall be put in place to ensure the physical security of the server room:

- Access to the server room shall be restricted to the authorized State Department staff only and a log, either biometric or otherwise shall be kept for such visits.
- Appropriate surveillance systems such as CCTV shall be installed.
- The server room shall contain adequate air conditioning and fire detection and suppression systems in order to provide a stable operating environment.
- Power feeds to the servers shall be connected through Un-interrupted Power Supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of server systems in case of power failure.
- Where possible generator power shall be provided to the server room to help protect the equipment in the case of a mains power failure.
- The server room floor shall be raised to protect equipment in the event of flooding

4.2.1.2 Networks

The State Department has established network infrastructure at the Headquarters and Missions. The following guidelines will be applied to safeguard these infrastructures: -

- LAN and WAN equipment such as switches, hubs, routers, and firewall shall be kept in secured rooms. In addition, the equipment shall be stored in lockable air-conditioned communication cabinets.
- Users shall not place or store any item on top of network cabinets.
- Where ducting is involved, fumigation and inspection shall be carried out regularly to curb damage to the cables by rodents.
- Personal wireless devices such as routers, switches shall not be connected to the network.
- Firewalls and Intrusion Detection systems shall be used across the entire network to monitor and prevent hackers, viruses and worms including all other forms of cyber-attacks.
- All computers hooked into the network shall mandatorily have an up-to-date antivirus software to prevent viruses and all other forms of malicious code.
- ICT shall deploy a Domain Controller to authenticate and validate users on the network, including group policies, user credentials, and computer names to determine and validate user access.

4.2.1.3 Handling of Computer Equipment and Accessories

The State Department has made deliberate effort to provide its members of staff both at the Headquarters and Missions with adequate ICT equipment and accessories to facilitate their work. These equipment and accessories should be handled with utmost care. Therefore, the following guidelines shall apply: -

- The State Department shall provide UPS to all ICT installations in order to protect the systems from power fluctuations and surge.
- Personal (own) Computers, Laptops and mobile devices shall not be used to store State Department data and information unless with express authorization by the Head of Department or Mission.
- Preventive maintenance shall be carried out twice a year to enhance performance and reduce equipment failure.
- Liquids shall not be placed on or near computer equipment as they can cause damage.
- Computers and other ICT equipment shall be properly shut down as required and never directly from power outlet.

4.2.2 Logical Security

4.2.2.1 Access Codes and Passwords

Access codes and passwords are critical in limiting access by unauthorized users to ICT resources. Maintaining security of the State Department's applications, email systems and network facilities are critical to providing data integrity and stability of the systems. Passwords are provided to limit access to these assets on need basis. The following guidelines will apply in ensuring adherence: -

- ICT Unit will be responsible for the administration of user IDs and all access codes to the networks and databases. Access to the systems will be provided upon receiving written communication from the respective Head of the Department/Mission owning the application.
- Limited user accounts will be provided for all non-staff who may need to access the State Department systems.
- Each user will take personal responsibility to protect and keep confidential all passwords issued to him/her by the State Department. Users should create strong passwords to prevent hacking through guessing. Passwords should be a combination of alphanumeric and special characters and at least eight characters long.
- Users are required to change their passwords at least every three (3) months.
- Accounts of all exiting staff will be deactivated.

4.2.2.2 Virus attacks

The State Department shall install necessary hardware and software such as antiviruses, firewalls in the servers and computers to deter malware which may cause destruction or damage to data. The software shall be configured for automatic updates. The following guidelines will apply:-

- Users should never disable the antivirus software for any reason.
- In case of suspected malware attack, users shall report to the ICT Unit for necessary intervention.

4.2.2.3 System and Data Security

The State Department is committed to protecting data and systems from misuse, unauthorized access, theft and environmental hazards. The State Department has a firewall to enhance security of systems and data. The following guidelines apply: -

- The State Department's data require proper management throughout its life cycle from creation to disposal or transfer to permanent archives. Users are not allowed to delete or transfer any official data stored in ICT equipment under their custody whether created by themselves or otherwise.

- Access, amendments and modifications to data will only be carried out strictly by authorized personnel and will be restricted in accordance with its nature, content and sensitivity.
- State Department data will be managed in line with State Department Records Management Policy.
- The State Department will deploy a data encryption system to secure stored data as well as data in transit.

4.3 RISK MANAGEMENT

Risk management is concerned with identification and management of threats that may affect the State Department's operations. The State Department like other organizations is faced with a number of risks including: operational risks occasioned by systems failures, Information security risks due to cyber threats, security breaches, malwares, viruses and user negligence.

Management of these risks is paramount in ensuring that ICT failures do not jeopardize the operations of the State Department. The State Department will implement the following measures to mitigate against these risks: -

- Conduct risk assessment on ICT infrastructure at the State Department headquarters and Missions abroad and take necessary preventive action.
- Conduct business analysis, feasibility studies/benchmarking exercises to avoid vendor driven projects.
- Conduct regular vulnerability and penetration tests.
- Conduct regular assessment of ICT Infrastructure and ensure timely maintenance.
- Adopt a variety of security solutions.
- Provide continuous training/sensitization of the State Department staff on information security.

CHAPTER 5

:INFORMATION TECHNOLOGY GOVERNANCE

5.1 IT GOVERNANCE

The role of Information Technology in leveraging an organization's competitive advantage cannot be overemphasized. The State Department like other entities seeks to achieve benefits from its investments in IT adoption and application. IT governance involves implementation of an IT framework that takes stakeholder, customer and regulatory interests into account. Internationally, there has been concerted effort to address IT governance by various professional bodies.

To achieve IT governance goals the State Department will optimize the resources available namely: information, services, infrastructure, applications and people's skills to manage the various risks. As part of good governance, the State Department will;

- Establish a Digitization Committee to provide oversight on ICT matters.
- Monitor the State Department's compliance with the set policies, legal, regulatory and contractual obligations.
- Align the State Department's ICT operations with national and international standards, best practices as well as code of conduct.
- Enforce the adoption of applicable Information Technology policies.
- Oversee successful implementation of this policy.

5.2 LEGAL, REGULATORY AND CONTRACTUAL COMPLIANCE

5.2.1 Background

Kenya is a signatory to a number of conventions and standards relating to ICT. Furthermore, Kenya's Missions abroad are not exempted from ICT Directives and Regulations applicable to their host country. Kenya Information and Communications Act, 1998, National Cybersecurity Strategy 2014; National Broadband Strategy 2018, Computer Misuse and Cybercrimes Act (CMCA), 2018, Data Protection Act (DPA), 2019, National ICT Policy Guidelines 2020 and National Digital Master Plan 2022 provides frameworks that guides e-services. To this end the State Department will implement the following measures in compliance with the above:

- Adopt and enforce relevant Cyber Security solutions.
- Provide Disability Friendly Information Technology services and equipment for its members of staff with disability.
- Sensitize State Department's users on acceptable use of Emerging Technologies.
- Enforce IT security controls.

5.2.2 Contractual Obligations

The State Department and its Missions relies on a number of firms for provision of ICT services. This calls for prudent management of suppliers and contracts, as well as sale/service agreements.

Provision of the services form a basis for a legal binding between the State Department/Mission and the service providers. Where the Mission outsources ICT services, it will ensure that the contractual obligations are honored in line with the applicable laws and regulations in the host country. The State Department will endeavor to;

- Negotiate for better deals aimed at providing services that offer value for money. Assess and document existing Service Level Agreements for effective management.
- Manage and monitor the implementation of Service Level Agreements.
- Facilitate prompt payment for services rendered to avoid disruptions.

5.2.3 Ethical Considerations

Though not enforced by any legal instrument, ethical issues play a major role in governance and management of Information Technology. Information leakages, careless utterances and opinionated posts on social media platforms by staff may have a far-reaching effect on the diplomatic relations, State Department's image and relationship with its stakeholders and publics. The State Department will put in place mechanisms aimed at promoting high ethical standards in the use of IT. This will include implementation of the guidelines provided in this policy in the earlier chapters.

CHAPTER 6

INSTITUTIONAL FRAMEWORK AND INSTITUTIONAL LINKAGES

6.1 INTRODUCTION

The successful implementation of this policy requires concerted effort and collaboration of various Government Departments and Agencies as well as private sector players and other partners. The State Department has identified the following institutional linkages and their corresponding responsibilities.

6.2 INSTITUTIONAL RESPONSIBILITIES

No.	Institution	Responsibility
1.	**Top Management: Cabinet Secretary and Principal Secretary**	□ Provide policy guidance and management support. □ Provide adequate resources to implement the policy □ Facilitate adequate staff of the ICT Unit including training of the personnel..
2.	**ICT Division**	□ Ensure coordination, implementation and compliance of the Policy. □ Provide support and guidance to users in understanding their roles and responsibilities in the implementation of the Policy.
3.	**Users: Missions, Directorates and Divisions**	□ Internalize and comply with the policy. □ Notify any breach of policy to the ICT Unit.
4.	**Ministerial ICT/Web management committee**	□ Oversee uploading/updating of content on Website in line with the policy. □ Membership will be drawn from Administration and Political Directorates. □ Govern IT issues in the State Department through evaluation of user needs, provision of direction through prioritization & decision making and performance monitoring and compliance.
5.	**State Department for ICT and ICTA**	□ Provide the requisite technical back stopping in the implementation of the Policy. □ Deploy adequate ICT personnel to the State Department. □ Provide policy guidance the management of website. □ Responsible for implementation of ICT standards.

6.	**The National Treasury**	□ Provide adequate budgetary provision to support policy implementation. □ Provide technical backstopping in the implementation of IFMIS. □ Provide technical backstopping in the implementation of e-procurement.
7.	**CBK**	□ Provide technical backstopping in the implementation of i-banking.
8.	**The Kenya Revenue Authority (KRA)**	□ Work closely with the Privileges Directorate to oversee implementation of the IPMIS component touching on tax and customs exemptions for Diplomats. □ Oversee compliance with statutory requirements such as tax compliance especially by Diplomats and international organizations.
9.	**NTSA**	□ Provide technical backstopping in the implementation of diplomats motor vehicle component of IPMIS.
10.	**The Directorate of Personnel Management (DPSM)**	□ Provide technical backstopping in the implementation GHRIS and IPPD. □ Facilitate staff deployment to ensure optimum staffing levels. □ Facilitate career progression.

CHAPTER 7

POLICY IMPLEMENTATION, MONITORING & EVALUATION

The successful implementation of this Policy hinges on three things: first, is a proper coordination framework defining the reporting and feedback channels; second, is adequate human resource capacity, and third is mobilization of financial resources. Consequently, the full involvement, effort and commitment of the State Department staff and all the stakeholders, will be critical for the State Department to realize the aspirations of this Policy. In this regard, the State Department will sensitize all staff on the Ministerial ICT Policy to ensure acceptance and hence build a critical mass for its successful implementation.

The Policy will form the basis for identification of State Department's annual targets to inform the preparation of annual work plans and budgets. In the current government reporting dispensation, the State Department monitors progress on its activities and evaluates performance through the preparation of quarterly and annual reports. Therefore, to ensure coherence in tracking results in the State Department, M&E will be undertaken using the existing M&E tools. An annual ICT Audit will also be undertaken to measure the successes and identify any shortcomings, as well as to determine the level of compliance with the policy, legal and regulatory requirements. M&E will provide useful feedback on the basis of which informed and evidence-based management decisions will be made.

Given that the ICT industry is one of the most dynamic sectors, the State Department will review the policy from time to time to respond to the changing technological advances and international environment.

HARAMBEE