REPUBLIC OF KENYA

The National Treasury & Planning

State Department for Planning

Information Security Policy

February 2022

Document Number: Version 1.1

VERSION HISTORY

DATE	VERSION	DESCRIPTION
January 2021	0	First Draft
25th January 2022	1	Revision and incorporation of comments from Directorates/Departments/Sections and Units
8th February 2022	1.1	Revision and incorporation of comments and suggested amendments by Economic Planning Secretary after peer review.

FOREWORD

I present to you the Information Security Policy, a document that shall guide the State Department for Planning in safeguarding information. This Policy takes into cognizance the provisions of the Government of Kenya laws, regulations, information technology standards and globally accepted best practices in ensuring appropriate security for information assets, including the data, technology, and processes within the domain of ownership and control of the State Department.

The Kenya Vision 2030 identifies ICT as a foundation for socio-economic transformation and enabler of a knowledge-based economy. It recognizes that knowledge plays a central role in boosting wealth creation, social welfare, and international competitiveness. Information and ICT technologies are essential in generating knowledge, making them assets to the Government, which must be secured by appropriate Policy and controls.

This Information Security Policy for the State Department for Planning shall not only endeavor to secure information assets but shall also contribute to effectiveness in delivering the desired vision and mission. This will assist the Country in joining the international community in the implementation of robust policies which facilitate factors that lead to foster socio-economic development and improvement of the living standards of the citizens.

The State Department is mandated to provide leadership and coordination in the formulation of National Development Policies and Programmes and tracking development results in the economy to ensure sustainable socio-economic development at the national and county levels. It is also responsible for designing and providing the required suitable plans and strategies that contribute to high and sustainable socio-economic development.

On the International Cooperation front, the State Department for Planning has enhanced Kenya’s position as a preferred investment destination through effecting a series of international and regional agreements on trade and investment financing.

In carrying out the State Departments’ mandate, information is an important asset that must be safeguarded. Therefore, a comprehensive Information Security Policy shall effectively influence the security norms and ensure the preservation of confidentiality, integrity, and availability of our information assets and systems through adherence to the set security protocols and procedures.

The Policy applies to both employees and all our stakeholders who, through our engagements and by the nature of their duties, have access to our information assets.

In a nutshell, this Policy, therefore, serves to ensure the effectiveness and efficiency of the State Department towards minimizing the risk of damage by preventing security incidents and reducing their potential impact on the Department's operations.

Saitoti

SAITOTI TOROME, CBS
PRINCIPAL SECRETARY, STATE DEPARTMENT FOR PLANNING

ACKNOWLEDGEMENT

The State Department for Planning set out to develop an Information Security Policy as part of the safety and security measures to safeguard personnel, documents, information, equipment, and other assets.

In the world today, information is considered a high-value asset and commodity, making it increasingly vulnerable to various security violations. Increased adoption of ICT to enhance business processes in Government has led to more information being converted into digital formats. The conversion of information into digital formats has made the information more susceptible to risks such as unauthorized access, use, disclosure, modification, and destruction.

Implementation of the Information Security Policy is aimed at protecting all types of Government information, regardless of whether it is in digital or hard copy form, from security threats and enforcing a security culture among the employees in the organization by helping them understand the risks to Government information in their daily work practices.

Developing the Information Security Policy has been consultative, involving various internal and external stakeholders. It is imperative to commend everyone whose contribution led to the development of this document, and I would therefore like to express my most profound appreciation to all those who made it possible.

Special gratitude goes to the Principal Secretary, Mr. Saitoti Torome, CBS, for his support and leadership in the development of the Policy. I would also like to express my sincere appreciation to the Economic Planning Secretary, Mrs. Katherine Muoki, OGW, whose input and review of the Policy has been instrumental. I would also like to commend the Safety and Security Measures Committee members for their dedication and hard work to develop the Policy. I would further like to extend my gratitude to the Directorates, Departments, Sections and Units whose input was invaluable towards ensuring the Policy facilitated the achievement of the organization's mandate.

The State Department also wishes to express deep appreciation to the Ministry of ICT, Innovation and Youth Affairs, and the ICT Authority in their critical role in guiding the development of this Policy and ensuring its alignment to Government laws, policies, and standards.

JOEL MAKORI
DIRECTOR ADMINISTRATION, STATE DEPARTMENT FOR PLANNING

LIST OF ACRONYMS AND ABBREVIATIONS

BYOD	Bring Your Own Device
DNS	Domain Name System
FTP	File Transfer Protocol
GCCN	Government Common Core Network
HOC	Head of Change
HOD	Head of Department
HR	Human Resource
HRPPM	Human Resource Policies and Procedures Manual
ICT	Information Communication and Technology
ID	Identification
IMAP	Internet Message Access Protocol
IS	Information Security
ISRM	Information Security Risk Management
IT	Information Technology
KNADS	Kenya National Archives and Documentation Services
LAN	Local Area Network
MAC	Media Access Control
PC	Personal Computer
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
POP3	Post Office Protocol version 3
RFC	Request For Change
SDP	State Department for Planning
SNMP	Simple Network Management Protocol
SSH	Secure Shell
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network

DEFINITION OF TERMS

Accounting Officer A public officer appointed to take full responsibility on the finances, assets and liabilities of the respective State Department, that is, the Principal Secretary.

Availability Having appropriate access to Information Assets as and when required in the course of the State Department’s operations.

Classified Information This is information that the Government deems to be sensitive information that must be protected through categorization into several (hierarchical) levels of sensitivity which include open, restricted, confidential, secret, and top secret.

Confidentiality The restriction of information to those persons who are authorized to receive or access it.

Co-opted member A member elected or nominated to be a part of the Information Security Committee based on knowledge and expertise in a particular operation of the State Department.

Information Data that has a meaning or can be interpreted. It can be held as an electronic record or non-electronic format such as paper, microfiche, photographs.

Information Asset Information that has value to the State Department for Planning. Critical Information Assets are the most important types of information required to achieve the SDP's strategic objectives.

Information Security It is a set of practices intended to safeguard data and information from unauthorized access or alterations during storage and when transmitted from one machine or physical location to another.

Information Security Unit Department/ Unit responsible for the function for Information Security within the State Department for Planning

Integrity The completeness and preservation of information in its original and intended form unless amended or deleted by authorized people or processes

Malware Malware is short for malicious software and refers to software specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Quality The state of completeness, validity, consistency, timeliness, and accuracy makes data appropriate for both operational and strategic use.

Third-Party Individuals or organizations who are not members of the State Department but are external parties with which it has a relationship. This may include both contractual and non-contractual parties.

TABLE OF CONTENTS

1. Introduction

The State Department for Planning (SDP) shall seek to enhance efficiency and effective service delivery to its stakeholders by reducing the probability of loss through the design and implementation of policies, standards, procedures, and guidelines that shall enhance the protection of business assets.

Information shall be classified and protected in a manner commensurate with its sensitivity, value, and criticality. Protection of information shall apply regardless of the media where the information is stored, the systems that process it, or the transmission mechanisms by which it is moved.

1.1. Background

Under the Performance Contract targets and guidelines, the State Department for Planning (SDP) is required to put in place measures to safeguard personnel, documents, information, equipment, and other assets guided by the Information Security Management System (ISMS) framework.

ISMS is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of ISMS is to minimize risk and ensure continuity of business operation by pro-actively limiting the likelihood and impact of a security breach. It addresses employee behavior and processes as well as data and technology.

Implementation of ISMS aims to protect all types of Government information, regardless of whether it is in digital or hard copy form, from security threats and enforce a security culture among the employees in the organization by helping them understand risks to Government information in their daily work practices. The framework for implementation of ISMS is based on the ISO/IEC 27001 international standard, which requires that organizations develop an Information Security Policy.

The Information Security Policy governs information protection, which is one of the many assets the Government needs to protect. The Information Security Policy is a set of rules enacted by the State Department to enable users of information systems, and the information stored and transmitted in/through them, to abide by the prescriptions regarding data and Information Security. It makes it possible to coordinate and enforce an Information Security program across the organization and communicate the security measure to internal and external stakeholders.

1.2. Policy Statement

The State Department is committed to preserving all its vital information assets' confidentiality, integrity, and availability to maintain its effective and efficient service delivery, legal and contractual compliance, and reputation. The Information Security framework (comprising this Policy, supporting policies, processes and tools, and the requisite management and decision-making structures) shall be an enabling mechanism for information sharing and reducing information-related risk to acceptable levels.

The Policy aims to protect the State Department's information assets against all internal, external, deliberate, or accidental threats.

This Policy contains various sub-policies which are:

1) Information Security Risk Management Policy.
2) Resource Management Policy.
3) Physical and Environment Security Policy.
4) Information and Communications Technology Policy.
5) Network Security Policy.
6) Information Technology Media Disposal Management Policy.
7) Electronic Information Transfer Policy.
8) Acceptable Use Policy.
9) Clear Desk/ Clear Screen Policy.
10) Bring Your Own Device(BYOD) Policy.
11) Identity and Access Management Policy.
12) Password Management Policy.
13) Network Access Policy.
14) Personnel and Awareness Policy.
15) Incident Management Policy.
16) Change Management Policy.
17) Business Continuity Management Policy.
18) ICT Disaster Recovery Policy.
19) Malware Management Policy.
20) Use of Cloud Services Policy.
21) Monitoring for Compliance Policy.

1.3. Policy Implementation Responsibilities

1) The Unit charged with the responsibility for Information Security Policy in the State Department is the executor of these Information Security policies.
2) All employees of the SDP and the relevant third parties shall be responsible for complying with the published policies.
3) Directorates, Departments, Sections and Units within the SDP have joint responsibility for monitoring continuous compliance with the policies herein.
4) The Information Security function shall respond to all inquiries on the policies contained herein.
5) The security of each system/asset shall be the responsibility of its custodian. The custodian is the person who is authorized to maintain and hold the information.
6) The responsibility for the overall coordination of Information Security lies primarily with the ICT Unit.

1.4. Rationale

Information is considered a high-value asset and commodity, making it increasingly vulnerable to various security violations. Increased adoption of ICT to enhance business processes in

Government has led to more information being converted into digital formats. The conversion of information into digital formats has made the information more susceptible to risks such as unauthorized access, use, disclosure, modification, and destruction. It is against this backdrop that the Information Security Policy is aimed at: -

1) Communicating the management direction and support for Information Security.
2) Defining what is required of the State Department's employees from a security perspective.
3) Providing direction upon which a control framework can be built to secure the organization against external and internal threats
4) Detecting and forestalling the compromise of Information Security, such as misuse of data, networks, computer systems, and applications.
5) Protecting the reputation of the State Department concerning its ethical and legal responsibilities
6) Providing a mechanism to hold internal and external stakeholders accountable for compliance with expected behaviors concerning Information Security.

1.5. Scope

This Policy covers the storage, access, transmission, and destruction of information in the course of the State Department for Planning operations. It also applies to the conduct of staff, stakeholders, and any other persons with access to that information (despite their location or the location of the information) as well as the applications, systems, equipment, and premises that create, process, transmit, or store information, whether in-house or provided by external suppliers.

1.6. Objectives

The main objective of this Policy is to protect the State Department’s information assets through safeguarding its confidentiality, integrity, and availability; specifically, the Policy aims to:

1) Protect the SDP's information assets through safeguarding its confidentiality, integrity, and availability.
2) Establish an effective Information Security governance structure, including accountability and responsibility for Information Security within the SDP.
3) Maintain an appropriate level of employee awareness, knowledge, and skill to minimize the occurrence and severity of Information Security incidents.
4) Ensure the SDP can continue and rapidly recover its business operations in a detrimental Information Security incident.
5) Ensure that staff, visitors, suppliers, and third-party providers are aware of and comply with all current and relevant Policy requirements and related legal and regulatory requirements.
6) Provide the principles by which safe and secure information systems working environments can be established for users, suppliers, third parties, and any other authorized users.

1.7. Policy Review

The Unit charged with the responsibility for Information Security in the State Department for Planning will initiate a review of these guidelines annually to ensure their appropriateness, responsiveness to the emerging Information Security risks, and compliance with legal and regulatory requirements.

2. Information Security Governance & Management

2.1. Introduction

The Information Security Governance and Management Policy aims to ensure that the State Department can plan, strategize, resource, and oversee the implementation and maintenance of Information Security functions within its scope of responsibility.

This Policy shall provide for an Information Security Governance and Management structure to ensure the SDP can provide strategic direction and align Information Security functions to the State Department's mandate.

2.1.1. Purpose

The aim of the Information Security Governance and Management Policy shall be:

1) To enable the establishment and provision of leadership for the Information Security function within the State Department for Planning.
2) To ensure efficient and effective implementation of this Information Security Policy.
3) To monitor, evaluate and report on the effectiveness of the Information Security Policy within the State Department.
4) To support decision-making and ensure continual improvement of Information Security practices within the State Department.

2.1.2. Scope

The Policy applies to the Information Security Governance and Management structure to be implemented by the State Department. The Authorized/Accounting Officer shall appoint an Information Security Committee chaired by the Head of the Administration Department with membership from Human Resource, ICT, and any other Department deemed necessary for the function. The ICT Unit shall be the Secretary to the Committee. The Committee shall meet whenever required to do so but not less than four times every financial year.

The Committee shall have the following terms of reference: -

1) To ensure that the objectives of the Policy are adhered to by all parties within the Policy admissibility scope.
2) To oversee all Information Security-related operations, projects and activities carried out within the State Department while ensuring the Policy requirements.
3) Facilitate appointment of Information Security champions team with involvement from users who are involved in promoting Information Security throughout the State Department.
4) To ensure that Information Security is entrenched into all the State Department's activities, including projects, service provider engagement, and recruitment.
5) To carry out any other duties delegated by the appointing authority relating to the Information Security function.

2.2. Roles and Functions of the Committee Members

The Information Security Committee shall report to the Accounting Officer, and the members shall have roles and responsibilities as follows: -

2.2.1. Officer in Charge of Administration

1) Convene and chair meetings.
2) Responsible for the timely production of Committee deliverables.
3) To provide leadership during crises or disasters.
4) Represent the interests of the premises and physical assets of the State Department.
5) Take responsibility for and report on the following systems and processes within the State Department:
   a) Classification of physical space to meet Information Security requirements.
   b) Management of boundaries/gates between physical areas of different categories.
   c) Physical access control systems.
   d) Spot checks and patrols of physical space.
   e) Physical incident management and recovery.

2.2.2. Officer in Charge of Human Resource

1) Serve as a member of the Committee.
2) Represent the interests of the staff, in particular, users of information systems.
3) Take responsibility for and report on the following systems and processes within the State Department: -
   a) Administration of Information Security compliance agreements with staff.
   b) Staff Information Security training and skills development.
   c) Information Security testing including monitoring of Human Resource (HR) compliance to Information Security Policy.
   d) Staff role rotation cycles.
   e) Rewards for Information Security performance and discipline for serious Information Security violations.
   f) Information Security job evaluation.

2.2.3. Officer in Charge of ICT

1) Act as the secretary of the meetings
2) Represent the interests of the Information Technology infrastructure, services, application, systems, and technical staff
3) Take responsibility for and report on the following methods and processes within the State Department: -
   a) Network administration.
   b) Database administration.
   c) Application administration.
   d) Information Security systems access management.
   e) IT service administration.
   f) Website, Email, and digital asset administration.

2.2.4. Co-opted Member

1) On appointment by the Chair, serve as a member of the Committee
2) Provide technical and institutional advice, help, and guidance in line with the requirements of the Chair for the duration set by the Chair
3) Carry out any other duties prescribed by the Chair and agreed by the Committee.

2.3. Information Security Organization Structure

2.3.1 The State Department for Planning shall establish an Information Security management structure that adequately responds to the security needs while ensuring the Department achieves its mandate in line with the vision.

2.2.2 The officer in charge of the Information Security function shall report to the Accounting Officer.

3. Information Security Risk Management

3.1. Introduction

This section provides a Policy for managing Information Security risk within the State Department. This begins with a risk assessment which should identify the Department's information assets, define the ownership of those assets and classify them according to their sensitivity and criticality to the Department. In assessing risk, Directorates, Departments, Sections and Units should consider the value of the asset, vulnerabilities and corresponding threats to that asset. Where appropriate, information assets should be labeled and handled following their criticality and sensitivity.

This Information Security Risk Management Policy covers the purpose, scope, application, Policy ownership, Policy, and Policy guidelines.

3.1.1. Purpose

To empower the office responsible for the Information Security function to perform periodic Information Security Risk Management (ISRM) to determine vulnerability areas and initiate appropriate remedies.

3.1.2. Scope

Information Security Risk Assessments shall be conducted on any Department/ Unit within the State Department or any outside entity that has signed a *Third Party Agreement* with the SDP. Information Security Risk Assessment shall be conducted on any information system, including data, applications, servers, networks, and any process or procedure by which these systems are administered and maintained.

3.1.3. Application

This Policy applies to all staff and stakeholders with access to the State Department for Planning data, information, applications and systems.

3.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the document Policy at regular intervals with the approval of the Accounting Officer.

3.2. Policy

The State Department for Planning shall develop an Information Security Risk Management Strategy to provide a structured risk identification, analysis, and appropriate risk management procedures.

3.2.1. The risk assessment shall consider existing legal and regulatory frameworks relevant to the State Departments mandate that could impact how it manages Information Security risks.

3.2.2. The State Department shall define the Risk Appetite (amount of risk that it is prepared to accept to achieve its' mandate) in terms of combinations of frequency and magnitude of a threat to absorb the loss, e.g., financial loss, reputation damage.

3.2.3. The State Department shall review and approve risk appetite and tolerance change over time, especially for new technology, new organizational structure, new business strategy, and other factors that require a risk assessment.

3.2.4. Information Security risk shall be addressed in project management regardless of the categorization of the project.

3.3. Policy Guidelines

Information Security Risk Management shall be undertaken as a broader enterprise risk management approach.

3.3.1. The execution, development, and implementation of remediation programs shall be the joint responsibility of the Department/Unit responsible for Information Security and the Department/Unit responsible for the system or area being assessed.

3.3.2. Employees are expected to cooperate fully with any risk assessment conducted on systems/processes for which they are accountable.

3.3.3. Employees are further expected to work with the Department responsible for ISRM to develop a remediation plan.

3.3.4. The risk assessment shall identify the Department’s information assets, define the ownership of those assets and classify them according to their sensitivity and criticality to the Department/Unit or SDP as a whole. In assessing risk, Departments should consider the value of the asset, the threats to that asset, and its vulnerability.

3.3.5. Where appropriate, information assets should be labeled and handled following their criticality and sensitivity.

3.3.6. Information Security Risk Assessment shall be conducted annually at planned intervals and on a need basis which the State Department’s operations may prompt.

4. Resource Management

4.1. Introduction

This section provides a Policy for managing information resources within the State Department. The State Department for Planning shall maintain and apply appropriate protective policies and procedures for help, including protecting records of business activities, applying Information Security classifications where applicable, controlling physical access to information assets, and controlling the use of information and communications technology. Resource management entails records security, Information Security classification, information asset register, and security of personal data.

This Resource Management Policy covers the purpose, scope, application, Policy ownership, the Policy addressing, Records Security, Information Security Classification, and the Information Asset Register.

4.1.1. Purpose

Ensure the office responsible for records management and owners of information assets maintains appropriate custody in line with the existing legal and regulatory frameworks.

4.1.2. Scope

Information shall take many forms including, but not limited to;

a) Hard copy data held on paper,
b) Data stored electronically in computer systems,
c) Communications sent by physical post or using email, and
d) Data is stored using electronic media such as USB drives, disks, and tapes.

4.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning information, systems and applications.

4.1.4. Policy Ownership

The owner of this Policy is the person in charge of Records Management. The person charged with the responsibility for Information Security shall facilitate reviewing the document Policy at regular intervals in collaboration with the person in charge of Records Management with the approval of the Accounting Officer.

4.2. Policy

The Policy provides for Records Security, Information Security Classification, and the Information Asset Register.

4.2.1. Records Security

The State Department for Planning shall:

4.2.1.1. Ensure the establishment of an active records management program and an identified person responsible for records management;

4.2.1.2. Ensure that staff maintains appropriate custody of records on behalf of the Government in line with the existing legal and regulatory frameworks;

4.2.1.3. Take into account legislation that is specific to its business operations when managing record security;

4.2.1.4. Ensure that records transfer and disposal is done in line with the existing relevant policies and regulations; and

4.2.1.5. Ensure appropriate access restrictions for all records according to the classifications in accordance with existing Policy frameworks.

4.2.2. Information Security Classification

Information Security classification includes all activities that ensure information is appropriately classified.

The State Department for Planning shall:

4.2.2.1. Ensure all information assets are assessed and classified by the owner according to their content. The classification shall determine how the document should be protected and who should be allowed access to it;

4.2.2.2. Ensure all information assets are assigned appropriate security classification and control following the existing regulations and policies;

4.2.2.3. Ensure that Information Security Classification schemes do not limit the provision of relevant legislation under which the State Department operates;

4.2.2.4. Ensure that security controls are proportional to the classification level, value, and degree of reliance on the information and systems; and

4.2.2.5. The State Department should provide information about how the information assets are classified.

4.2.3. Information Asset Register

The asset protection responsibility domain includes all activities that implement and maintain appropriate protection of SDP information assets.

4.2.3.1. The State Department shall maintain the security of classified record/information asset registers to record details of each classified asset.

4.2.3.2. Security classified record registers may be part of an overall information asset register or managed separately. The register itself is an information asset that should be classified.

4.2.3.3. All ICT assets that create, store, process, or transmit classified information shall be assigned appropriate controls following the Government of Kenya Security manual.

4.2.3.4. All ICT assets should be identified, documented, and assigned asset custodians to maintain security controls.

4.2.3.5. All ICT assets that provide underpinning and ancillary services shall be protected from internal and external threats (e.g., mail gateways, domain name resolution, time, reverse proxies, remote access, and web servers).

5. Physical and Environment Security

5.1. Introduction

This section provides a Policy for managing physical security within the State Department. Physical security refers to protecting personnel, ICT hardware, software, networks, information and data from physical actions and circumstances that could cause severe loss or harm. Controls shall be adopted to lessen the risk of potential environmental threats to the information processing facilities and other ICT assets.

This Physical and Environment Security Policy covers the purpose, scope, application, Policy ownership, the Policy addressing general physical security, cabling, controlling access to buildings, removal of equipment and safety of off-site equipment, and equipment maintenance.

5.1.1. Purpose

The purpose of this Policy is to control physical access to the State Department's Information Technology, hardware, and systems to reduce the risk of damage to these critical resources. Damages include the breach of sensitive information and intellectual property, compromised system confidentiality, availability, or the corruption of information integrity.

5.1.2. Scope

This Policy covers ICT infrastructures, including data centers, ICT labs, equipment, network cabling, and end-user devices in the State Department.

5.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

5.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the document Policy at regular intervals with the approval of the Accounting Officer.

5.2. Policy

ICT equipment and all other information system components shall be installed in suitable protected areas (inside or outside the building) with minimal indication of their purpose and presence to preserve confidentiality, integrity, and availability of data and information.

The following controls shall be implemented:

5.2.1. General Physical Security

5.2.1.1. Whenever possible, doors and entrance locations of facilities shall be locked when unattended and protected during non-business hours by electronic alarms.

5.2.1.2. A record of the users of physical access controls such as facility keys shall be kept.

5.2.1.3. A record of security-related repairs and modifications, such as hardware, walls, doors, and locks, to a section containing protected information assets, shall be kept.

5.2.1.4. Private desk drawers, personal computers, peripherals, and related equipment shall be locked when not in use.

5.2.1.5. Back-up media shall be located off-site to avoid damage from a disaster on the State Department for Planning.

5.2.1.6. Protection shall be implemented against fire, flood, and other environmental factors that could damage the resources.

5.2.1.7. Access to/use of publicly accessible network jacks shall be restricted.

5.2.1.8. Emergency power shutdown controls shall be installed where applicable.

5.2.1.9. Equipment shall be located on racks raised above floor level.

5.2.1.10. Testing and servicing shall be performed on all fire and protective systems periodically.

5.2.1.11. Environmental controls shall be implemented to ensure that temperature and humidity are maintained within limits for the equipment contained therein.

5.2.1.12. Electrical power for servers shall be protected by Uninterruptible Power Supplies (UPS) to ensure continuity of services during power outages and protect equipment from damage due to power irregularities.

5.2.1.13. Each UPS should have sufficient capacity to provide at least 15 minutes of uptime to the systems connected to it to facilitate the graceful shutdown of equipment.

5.2.1.14. Computing devices shall be fitted with effective surge protectors to prevent damage to data and hardware caused by power spikes.

5.2.1.15. Secured access devices (e.g., access cards, keys, combinations, etc.) shall not be shared by authorized users or loaned to others.

5.2.2. Cabling

5.2.2.1. In line with industry electrical / cabling standards, precautions shall be taken to mitigate the risk of unauthorized/malicious data interception and accidental/malicious damage to ICT installations.

5.2.2.2. Electric cabling shall be physically separated from data cabling to prevent interference and reduce the risk of injury and damage to equipment.

5.2.2.3. All power and telecommunications lines into information processing facilities shall be installed underground and subject to adequate protection.

5.2.2.4. All cabling and networking equipment shall be clearly labeled using a documented convention to minimize handling errors.

5.2.2.5. All communications or networking equipment (routers, switches, hubs, and patch panels) shall be protected against unauthorized physical access by either placing it within a secured data center or a locked cabinet or room.

Specific requirements for the Data Center:

a) Comply with all requirements listed above.
b) The Data Center shall be located in a secure environment protected by keys or card access controls to mitigate unauthorized access and use.
c) Data Center access shall be restricted to only authorized personnel and authorized third parties when escorted.
d) Fire suppression equipment shall be installed within the Data Center.

5.2.3. Controlling Access to Buildings

5.2.3.1. Third-party support services personnel shall be granted access to secure areas only when authorized and supervised.

5.2.3.2. Physical access to the building by the public shall be subject to security screening.

5.2.3.3. An inventory of anyone accessing the SDP's building with a personal computer shall be kept on entrance and exit.

5.2.3.4. Badges shall be designed to distinguish visitors and employees. Temporary badges must expire after a pre-determined period.

5.2.3.5. Badges shall be carried by employees, internal contractors and displayed by third-party contractors or visitors.

5.2.3.6. All employees, contractors, vendors, and visitors shall immediately report any lost identification badges to the SDP and inform the SDP Customer Service Desk.

5.2.3.7. Employees shall be required to notify SDP security of any suspicious personnel within SDP's secure areas.

5.2.3.8. Physical access rights must be removed or disabled as soon as possible when an employee, contractor, or visitor no longer needs access due to changing roles or leaving SDP's premises.

5.2.3.9. The Department's supervisor will regularly review physical access rights, who initially approved access to SDP premises. This review shall be conducted annually.

5.2.4. Removal of Equipment and Security of Off-Site Equipment

5.2.4.1. Employees and contractors shall not remove property (except personal mobile devices) from SDP premises without prior authorization.

5.2.4.2. An inventory of all ICT assets must be maintained, which lists equipment that has been removed from SDP premises.

5.2.4.3. SDP's employees who travel with laptops or other equipment with "Sensitive" information, including portable hard drives must be cautious and shall take responsibility for keeping the items and information secure.

5.2.4.4. Security mechanisms (strong authentication and encryption) shall be implemented on portable devices according to the classification of the data stored on each machine according to the Data Classification Standard.

5.2.4.5. All storage media taken off-site by service providers (such as faulty disk drives and tapes) requires specific physical management and destruction procedures, as described in the Data Classification Standard.

5.2.4.6. Information Security assets shall only be moved from one location/Department to another only when authorized.

5.2.5. Equipment Maintenance

5.2.5.1. All information assets shall be regularly monitored and maintained following the manufacturer's specifications.

5.2.5.2. All regular maintenance activities shall be documented in the operational documentation of the Information system components. The documentation includes the frequency and details of routine maintenance that shall be performed.

5.2.5.3. SDP Management shall make available to the Officer responsible for Information Technology/Information Security/Data Centre manager the following:

5.2.5.3.1. The equipment maintenance schedule that depicts the activities to be conducted and the contact details of the individuals, including third parties who shall be performing the maintenance work.

5.2.5.3.2. The maintenance reports that describes the activities completed, any problems identified, and the respective problem resolution activities.

5.2.5.3.3. Only authorized maintenance personnel shall be allowed to perform repairs. The Officer in charge shall grant the maintenance personnel outlined in the maintenance schedule.

6. Information and Communications Technology

6.1. Introduction

This section provides a Policy for managing information and communications technologies within the Department. Information and Communications Technology includes activities that ensure appropriate resource management procedures, specifically relating to Information and Communications Technology (ICT).

This Information and Communications Technology Policy covers the purpose, scope, application, Policy ownership, operational procedures and responsibilities, third-party service delivery, and backup procedures.

6.1.1. Purpose

SDP shall implement and maintain a comprehensive set of Information Security controls relating to ICT that meet requirements identified by a risk assessment.

6.1.2. Scope

SDP shall refer to the Government of Kenya ICT Policy and Information Security Standards regarding Information Security controls relating to ICT implementations.

SDP shall implement detection, prevention, and recovery controls to protect against malicious software.

6.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

6.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer.

6.2. Policy

This Policy covers the operational procedures and responsibilities, end-user device Policy, third party service delivery and backup procedures.

6.2.1. Operational Procedures and Responsibilities

Operational procedures and responsibilities include all activities that ensure information processing facilities are secure.

The State Department for Planning shall:

6.2.1.1. Ensure operational procedures and controls are documented and implemented to ensure that all information assets and ICT assets are managed securely and consistently (following the level of security required); and

6.2.1.2. Ensure operational change control procedures are implemented to ensure that changes to information processing facilities or systems are appropriately approved and managed.

6.2.2. Computing Devices Policy

This Policy establishes security requirements for end-user and other computing devices which include servers, desktops and laptops. These devices may be issued by the State Department to facilitate staff in carrying out their duties or responsibilities or used to host or access SDP data, information, systems and network.

To reduce the Information Security risks:

6.2.2.1. The device shall be secured using appropriate access control credentials as defined in the Identity and Access Management and Password Policy.
6.2.2.2. The device shall be assigned to an owner who will be responsible for safeguarding the device and preventing unauthorized access.
6.2.2.3. Appropriate operating systems hardening configurations shall be implemented on the devices according the Computer Systems Hardening Procedures Manual.
6.2.2.4. The ICT Unit shall ensure that computing devices have corporate-approved anti-virus software installed, enabled and configured.
6.2.2.5. End-users shall ensure that they run regular operating system updates on the Computer devices.
6.2.2.6. Computing devices shall only have software installed from trusted source.
6.2.2.7. Loss of any device must be reported to the State Department.
6.2.2.8. Employees shall ensure regular back up of data and information in their devices belonging to the State Department.

6.2.3. Third-Party Service Delivery Policy

This Policy establishes security requirements for using ***third parties*** that handle SDP ***confidential*** information by storing, processing, transmitting, or receiving data.

To reduce the Information Security risks associated with contracted services and staff, SDP shall:

6.2.3.1. Identify risks related to ***third parties*** to ensure appropriate protection of SDP ***information assets;***
6.2.3.2. Define Information Security requirements for third-party agreements;
6.2.3.3. Ensure third-party information management oversight from contract initiation through termination;
6.2.3.4. Evaluate the third party's use of other third parties (i.e., subcontracting relationships) technology to support the contracted operations;
6.2.3.5. Evaluate the experience of the third party in providing services that include the handling of confidential information in the anticipated operating environment;

6.2.3.6. Evaluate the third party's ability to respond to service disruptions (see Incident Management and Business Continuity and Disaster Recovery policies);

6.2.3.7. Determine whether the third party provides sufficient security precautions, including, when appropriate, firewalls, encryption, and customer identity authentication, to protect SDP information resources as well as to detect and respond to intrusions;

6.2.3.8. Evaluate whether the SDP has complete and timely access to its information maintained by the third party both during and after any third party engagement;

6.2.3.9. Evaluate the third party's knowledge of regulations that are relevant to the services they are providing;

6.2.3.10. Ensure the third-party service delivery agreements complies with the Policy; and

6.2.3.11. Ensure third-party service delivery agreements are periodically reviewed and updated to address any changes in business requirements but remain compliant with the Policy.

6.2.4. Backup Procedures

6.2.4.1. Backup procedures include all activities that maintain the integrity and availability of information and applications through backup activities.

6.2.4.2. SDP shall develop and implement a comprehensive information and system backup program.

7. Network Security

7.1. Introduction

This section provides a Policy for security of the network within the State Department. The network security domain includes all activities that ensure the safety of information being transmitted over the network.

The Government has embraced the information age and widely utilizes interconnectivity between networks, particularly connectivity to the Internet. This exposes its non-public networks to a hostile environment of rapidly evolving threats. Connections to other networks provide convenient channels through which external parties can attack and damage Government systems. In addition, internal network users can deliberately or inadvertently threaten the network and its endpoints through their actions.

This Network Security Policy covers the purpose, scope, application, Policy ownership, and procedure.

7.1.1. Purpose

This Policy aims to provide guidelines for securing connections to the State Department for Planning corporate network.

The State Department's network and its computing resources (hardware and software) are owned by the Government of Kenya. They are provided to support the business processes and functions of the Government. The purpose of this Policy is to keep a high standard of network security. Adherence to the Policy shall help protect the integrity of the Government network and networked data. Enforcement actions shall mitigate risks and losses associated with security threats to the network and networked data. This Policy provides guidelines and procedures to govern the use of equipment and technologies and help ensure effective network management. Directorates, Departments, Sections and Units may adopt additional rules and regulations to meet specific administrative or business needs. Any adopted requirements must comply with this Policy.

7.1.2. Scope

This Policy applies to all State Department for Planning employees, contractors, consultants, temporary staff, and other workers, including personnel affiliated with third parties utilizing and accessing the State Department’s network.

Authority for exemption or non-compliance can be granted by the Accounting Officer in case of any network security concerns.

7.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

7.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer.

7.2. Policy

The State Department shall provide network security capabilities at a reasonable and appropriate level for the nature of the data being transmitted. The State Department must ensure that access to information assets is restricted to authorized personnel and protected at all times.

7.2.1. Network confidentiality: The State Department shall implement encryption and device authentication controls to protect transmitted information.

7.2.2. Boundary protection: The State Department shall establish internal controls that monitor and control the flow of information within and at the external boundary.

7.2.3. The Head of ICT shall designate an Officer responsible for managing and administering network boundary protection strategies.

7.2.4. The Boundary Protection strategies shall include but are not limited to:

a) Physical Security: The State Department shall employ due diligence in ensuring physical security at any location where boundary protection devices are installed.

b) Access Control: All access to State Department information systems and networks shall be controlled and monitored according to the Access Control Policy.

c) Interconnections: All connections to information systems outside the security boundary of the State Department or the state backbone (internet, or other external network or information system) shall be fully documented, authorized, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels) and be continuously monitored.

d) Adopt most minor functionality: Network boundary control devices managed by the State Department shall be configured to provide essential capabilities and prohibit and restrict the use of functions, ports, protocols, and services that are not in use.

e) Monitoring: The State Department shall also monitor for inappropriate use of network services.

7.2.5. Network Documentation: The State Department's network architecture shall be documented, including internal and external network connections. The network documentation shall be reviewed and updated annually or when major network or systems revisions are implemented. The documents, including network diagrams, routing tables, and IP addresses, shall be classified as confidential and protected accordingly.

7.2.6. Configuration Changes: All changes to network configuration parameters shall be authorized by the officer responsible for the Information Security system and documented following change control policies and procedures. Privileges to modify the functionality, connectivity, configuration, and services supported by the network shall be restricted to the authorized designee(s). A formal process for approving and testing all network configurations shall be implemented.

7.2.7. Network Device Hardening: The State Department shall implement network device hardening in line with the Government Information Security Standards with minimum security baselines defined, including the business justification for the use of services, protocols, and ports allowed for system components, specifically security features implemented for those protocols considered to be insecure (e.g., FTP, Telnet, POP3, IMAP, and SNMP). In collaboration with the Department managing the Government network, the State Department shall block ports and services if an event is identified that could adversely impact the network.

7.2.8. Wireless Connections:

a) Installation of any wireless access or routing devices shall be done through the ICT Unit and in collaboration with the Department responsible for managing the Government Network. Wireless access and routing devices not owned and operated by the State Department or the Department responsible for managing the Government Network are not permitted to connect to the State Department's secured wired or wireless network.

b) All users shall authenticate to use the State Department’s secure wireless connections.

c) There shall be no open access to the State Department’s wireless connections.

d) Visitor wireless access points shall not be permitted to access the State Department’s network.

e) The State Department’s personnel shall not concurrently connect to the Department's wired infrastructure and any wireless network not belonging to the State Department or the Department responsible for managing the Government Network.

f) All wireless infrastructure devices that reside at the State Department or connect to the Department’s network shall maintain a hardware address (i.e., MAC address) that can be registered and tracked. Audit of wireless access points shall be carried out quarterly to detect any unauthorized access points.

7.2.9. Remote Access Security Management: All remote access connections into the State Department’s internal networks shall be established through approved methods.

a) All external connections to the State Department’s networks shall be reviewed and approved by the Accounting Officer and Head of ICT.

b) All external connections to the State Department’s network shall be documented.

c) Remote access shall only be provided if the appropriate approvals support a business need.

d) Remote connections shall be achieved by approved, secure remote access solutions such as VPNs with appropriate access control restrictions, and authentication must be implemented.

7.2.10. Secure File Transfer: Users shall use State Department-approved secure file transfer solutions to protect data from interception, unauthorized copying, unauthorized modification, misrouting and unauthorized destruction. Information and data shall be encrypted during transfer. File transfer solutions shall conform to the password Policy for authentication.

7.2.11. Network Monitoring and Logs: The State Department shall continuously monitor the network and corresponding network devices for suspicious activity and inappropriate use and utilize the logging capabilities following the log management policies and standards. The officer charged with the responsibility of Information Security shall alert the Head of ICT of suspected compromises for relevant corrective measures and escalation to be undertaken.

7.2.12. Denial of Service, Intrusion Detection, And Malicious Code: The State Department shall ensure boundary protection controls protect and monitor the network against malicious code, denial of service, intrusions, and other hacking attacks. For systems threats categorized as MODERATE or higher, a notification alert shall be sent to the ICT Authority Information Security Unit for further intervention.

7.2.13. Record Retention: All documentation and network logs shall be retained following the State Departments' retention policies and schedules. No specific retention requirements are set forth by this Policy.

7.2.14. Periodic Review: Network configurations shall be reviewed to ensure compliance with the State Department's policies. Supporting documentation shall exist for all enabled services. The State Department is responsible for testing its network configurations for effectiveness.

7.2.15. Security Updates: The State Department's personnel responsible for managing the network shall subscribe to security advisories and other relevant sources providing up-to-date information about network vulnerabilities and apply appropriate patches, updates, and other recommended protective actions.

7.2.16. Contingency Planning: The State Department, in collaboration with the Department responsible for the Government Common Core Network (GCCN) network, shall take appropriate measures to determine the degree of redundancy based on availability requirements for the affected data and put in place applicable effort in line with the Business Continuity Policy.

7.2.17. Network configurations implemented by the State Department shall be backed up entirely, a redundancy and failover strategy shall be employed, and alternate processing sites shall provide adequate protection.

7.2.18. Network Access: The State Department shall establish controls to manage and mitigate the risks associated with network connections. Additionally, the State Department shall ensure that:

a) Physical access to network devices owned by the Department are controlled and monitored.

b) Users are only provided with access to the services that they have been specifically authorized to use.

c) Access to the State Department's network and network resources requires the use of Government-issued identification and authentication credentials.

d) Access and use of the State Department's networks shall be following the appropriate use and access control Policy.

e) Service networks that carry sensitive applications shall be isolated from the rest (Internet) to eliminate co-mingling.

7.2.19. Network Addresses Management: The State Department's ICT Unit shall be responsible for issuing, managing, and approving IP addresses regarding any equipment to be plugged into the network in collaboration with the Department charged with the responsibility of managing the Government Common Core Network (GCCN). Disclosure of private IP addresses and routing information to unauthorized entities are forbidden.

7.2.20. Incorporation of Network Security Controls: The State Department's ICT Unit must put in place network security controls in collaboration with the Department charged with managing GCCN.

7.2.21. Authentication of Users: The State Department's ICT Unit must put controls for the authentication of users.

7.2.22. Training of Users: The State Department's ICT Unit shall educate users to create awareness and minimize the risks of attack or compromise while providing proper functionality and performance.

7.2.23. Registration and Authentication of Devices: Appropriate controls must be put in place to mitigate intrusions associated with instruments which include but are not limited to portable storage devices, laptops, Personal Digital Assistant (PDAs) and tablet PCs, switches, routers, and computers. The State Department's ICT Unit shall register and authenticate various devices for connection to the network.

7.2.24. Acceptable Connection Methods: The State Department's ICT Unit shall ensure that remote connections go through approved Virtual Private Networks (VPNs) or Secure Shell (SSH) tunnels. Extending or modifying the GCCN networks should be done with notification and approval by the Department charged with managing the GCCN network.

7.2.25. Vendor Defaults: All vendor defaults, including but not limited to default encryption keys, administrator usernames, passwords, and SNMP commUnity strings, must be changed.

7.2.26. Domain Name System (DNS): The State Department shall ensure that all official domain names for systems are registered through the organization charged with managing Government domains.

a) Virtual Private Networks (VPNs): The State Department's personnel and authorized third parties (customers, vendors, etc.), where applicable, may utilize the benefits of VPNs to access the Department's network and information systems security.

b) Personnel with VPN privileges are responsible for ensuring that their credentials are not disclosed to prevent unauthorized users from accessing the State Department's internal networks.

c) VPN access shall be controlled using solid passwords, token devices where applicable and other measures defined in the password Policy.

d) VPN gateways shall be set up and managed in consultation and collaboration with the Department responsible for managing the GCCN network.

e) All computers connected to the State Department’s internal networks via VPN or any other technology must use the most up-to-date anti-virus software provided by the State Department; this includes personal computers.

f) VPN users shall be automatically disconnected from the State Department's network after thirty minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes shall not be used to keep the connection open.

g) Users of computers that are not State Department for Planning-owned equipment must have their equipment configured to comply with State Departments’ VPN and network policies.

h) The State Department shall approve all VPN clients to be used. Only authorized VPN clients may be used.

i) Using VPN technology with personal equipment makes users understand that their machines are a de facto extension of the State Department's network. As such are subject to the same rules and regulations that apply to State Department-owned equipment, i.e., their machines must be configured to comply with Information Security Policies.

8. Information Technology Media Disposal Management

8.1. Introduction

This section provides a Policy for management of Information Technology storage media disposal within the Department. Disposal entails the removal of media off-site under warranty or hardware service agreements. Unauthorized use of information can occur through careless disposal hence the need for secure media management.

This Information Technology Media Disposal Management Policy covers the purpose, scope, application, Policy ownership, and the approach which focuses on the disposal of information technology media.

8.1.1. Purpose

To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

8.1.2. Scope

The Policy addresses secure management of removable media, disposal of information storage media, and physical media transfer.

8.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

8.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer.

8.2. Policy

8.2.1. The SDP shall develop and implement secure storage media disposal procedures in collaboration with the Supply Chain Management Unit.

8.2.2. When disposing of media, SDP shall ensure all information held on the media is either retained or disposed of in a secure fashion and accordance with the Public Procurement and Asset Disposal Act, 2015 and;

8.2.3. Computing hardware (e.g., computers) shall be disposed of following the relevant disposal regulations and standards.

8.2.4. SDP shall address the need for sanitization or destruction of media before reuse in a new environment or disposal. The State Department shall develop and approve Media Sanitization and Disposal Guidelines.

8.2.5. SDP shall use equipment endorsed/ allowed by the Government of Kenya.

9. Electronic Information Transfer

9.1. Introduction

This section provides a Policy for Electronic Information Transfer within the Department. The information exchange domain includes all activities that maintain the security of information exchanged internally and externally.

This Electronic Information Transfer Policy covers the purpose, scope, application, Policy ownership, and the approach which addresses email account creation, retention, deletion, and general standards.

9.1.1. Purpose

To ensure methods for exchanging information within the State Department, between the State Department and Ministries, Departments, Agencies and Counties, through online services, and with third parties are compliant with this Policy and applicable legal and regulatory frameworks.

9.1.2. Scope

This Policy covers the electronic mail (e-mail) and instant messenger correspondences and applies to all staff and stakeholders operating on behalf of /with the SDP.

9.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

9.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the document Policy at regular intervals with the approval of the Accounting Officer.

9.2. Policy

9.2.1. Email Account Creation

All SDP staff members shall receive official email accounts upon deployment. This shall be in line with the approved internal email account provision procedures.

9.2.2. Email Correspondences and Retention

This Policy covers all incoming or outgoing correspondences as well as their retention.

9.2.2.1. Administrative Correspondence

9.2.2.1.1. SDP Administrative Correspondence shall include incoming/outgoing and internal correspondence about the formulation, planning, implementation, interpretation, modification, or redefinition of the programs, services, or projects of the State Department.

9.2.2.1.2. All emails with the "Management Only" information sensitivity label shall be treated as administrative Correspondence. An email address shall be created to ensure the Administration Department retains Executive Correspondence. If a copy (cc) is made to this address, retention shall be administered by the ICT Unit.

9.2.2.2. **Financial Correspondence**

SDP Financial correspondence shall be all information related to financial matters for the State Department. An email address shall be created to ensure the Finance Department retains financial correspondence. If a copy (cc) is made to this address, retention shall be administered by the ICT Unit.

9.2.2.3. **Departmental Correspondence**

Directorates, Sections, and Units shall each have official email addresses retained by the specific offices.

9.2.2.4. **General Correspondence**

General Correspondence shall cover information related to customer interaction and the operational decisions of the State Department. The individual employees shall be responsible for email retention of General Correspondences.

9.2.2.5. **Ephemeral Correspondence**

9.2.2.5.1. SDP Ephemeral Correspondence shall include:

a) Documents of a routine or trivial nature;
b) Records which duplicate (or extract) information which is already held elsewhere; and
c) Documents with little or no administrative, fiscal, legal, evidential, cultural, or known historical value.

9.2.2.5.2. Short Correspondence shall be retained by the specific Directorate/Department/Unit/Section/Individual for a necessary period.

9.2.2.6. **Instant Messenger Correspondence**

9.2.2.6.1. SDP Instant Messenger General Correspondence shall be saved with the logging function of Instant Messenger or copied into a file and saved.

9.2.2.6.2. Instant Messenger Administrative or Fiscal Conversations shall be copied into an email message and sent to the appropriate email retention address.

9.2.2.7. **Encrypted Communications**

SDP encrypted communications shall be stored consistent with the Information Security Policy, but the information shall be generally kept decrypted.

9.2.3. Email Forwarding

Blanket forwarding of SDP email to internal and external accounts shall not be permitted. The email account is only for official use by staff.

9.2.4. Recovering Emails

SDP shall maintain a backup of official emails in line with the backup Policy.

9.2.5. Email Account Deletion

Staff who leave the State Department shall no longer have access to their SDP email account. The staff member's departmental head or immediate supervisor shall access their email account for 30 days to facilitate retrieval of official documents or information. After that time, the email account shall be deleted unless a request is made to the SDP ICT Unit to extend this period.

9.2.6. General Standards

9.2.6.1. Approved Electronic Mail

SDP shall use approved emails provided by the relevant Department responsible for emails creation, and the ICT Unit shall manage the emails.

9.2.6.2. Approved Encrypted email and files

All SDP emails shall be encrypted as per the Encryption guidelines.

9.2.6.3. Approved Instant Messenger

All Instant Messenger software used shall align with this Policy and any other related SDP Policy.

9.2.6.4. Individual Access Controls

Individual Access Controls shall be restricted to individuals’ accounts.

9.2.6.5. Insecure Internet Links

All SDP emails shall be accessed via secure Internet Links.

10. Acceptable Use

10.1. Introduction

This section provides a Policy for acceptable use of ICT within the Department. The procedure is to define fair use of the State Department’s ICT resources, including applications, hardware, information, and other information technology-based resources and systems. ICT resources play a more integral role in facilitating the SDP to achieve its mandate. Thus policies must be put into place to protect their confidentiality, integrity, and availability thus facilitating the SDP management, staff, and stakeholders enhance service delivery.

This Acceptable Use Policy covers the purpose, scope, application, Policy ownership, and the approach which addresses internet usage, computer access control, email, and ICT equipment.

10.1.1. Purpose

This Policy aims to define the appropriate usage of ICT resources by State Department for Planning employees and its stakeholders.

10.1.2. Scope

The purpose of this Policy is to outline the acceptable use of ICT equipment and information assets at the State Department, password use, physical and environmental security, computer access control, Internet and email conditions of use, clear desk and clear screen Policy, mobile storage devices, and software.

10.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

10.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer.

10.2. Policy

10.2.1. Internet usage

The Internet Usage Policy applies to all users (individuals working for the State Department including permanent, temporary, casuals, interns, and attaches) who access the internet through the networking resources. The Organization's internet users are expected to be familiar with and comply with this Policy and exercise their good judgment while using Internet services.

Internet Services Allowed

10.2.1.1. Internet access is to be used for the achievement of organization deliverables only.

10.2.1.2. Internet access shall be provided to users to support SDP activities and only as needed to perform their jobs.

10.2.1.3. Users shall not;

a) Use the internet to make personal gains or conduct a private business.
b) Use the internet to gamble.
c) Place any information on the internet that relates to SDP, alter any information about it, or express any opinion, unless they are expressly authorized to do so.
d) Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval.
e) Download any software from the internet without prior approval from the ICT Unit.

10.2.2. Computer Access Control

Individual responsibility access to the SDP systems is controlled by user IDs/accounts, passwords, and tokens. All User IDs/accounts and passwords are to be uniquely assigned to named individuals, and consequently, individuals are accountable for all actions carried out on their computers.

Individuals shall not:

10.2.2.1. Allow anyone else to use their user ID/token/account and password to access any systems used in SDP or leave their user accounts logged in at an unattended and unlocked computer.

10.2.2.2. Leave their password unprotected (for example, writing it down).

10.2.2.3. Attempt to access data they are not authorized to use or access.

10.2.2.4. Give or transfer data or software to any person or organization outside SDP without the authority.

10.2.3. Email

The use of email is intended for SDP communication. Personal use is permitted where such use does not affect the individual's performance and is not detrimental in any way. Personal service is also allowed where such use does not breach any term and condition of employment and does not place the individual or SDP in breach of statutory or other legal obligations.

Individuals shall not:

10.2.3.1. Use the email for harassment or abuse.

10.2.3.2. Access, download, send or receive any data (including images), which SDP considers offensive and defamatory in any way.

10.2.3.3. Use the email to make personal gains or conduct personal business.

10.2.3.4. Use the email systems in a way that could affect their reliability or effectiveness, for example, distributing chain letters or spam.

10.2.3.5. Send unprotected sensitive or confidential information externally.

10.2.3.6. Make official commitments through email on behalf of, unless authorized.

10.2.4. ICT Equipment

This includes all front end (laptops, computers, photocopiers, printers) and back end (servers, network switches, and firewall). All this equipment must be preserved and protected for the purposes they were obtained.

10.2.4.1. Employees shall utilize a computer, printer, or another computing device related directly to the daily operation.

10.2.4.2. Employees shall not utilize a computer, printer, or another computing device to engage in any activity that is in any way illegal or violates the SDP mandate or IS Policy.

10.2.4.3. Employees shall not use a computer to create, view, display, or store any document, picture, video, or other electronic file containing unauthorized content,

10.2.4.4. Employees shall not use SDP printers to print incidental and occasional personal documents.

10.2.4.5. Upon retirement, transfer, or dismissal, the user shall ensure that all ICT equipment are returned.

10.2.4.6. The user shall report the loss or theft of ICT Equipment they are responsible for.

10.2.4.7. Users must keep ICT equipment (Mobile devices) in their possession within their sight whenever possible. Mobile ICT equipment should never be left visibly unattended unless suitably secured.

10.2.4.8. The user shall ensure that mobile devices are regularly connected and logged onto the network to receive security updates at least monthly.

10.2.4.9. Users shall not share their official ICT equipment, e.g. laptops, with friends or family members.

10.2.4.10. Users shall not sell or dispose of ICT equipment without authorization.

11. Clear Desk/ Clear Screen

11.1. Introduction

This section provides a Policy on maintaining a clear desk and clear screen within the State Department. The Policy refers to practices meant to ensure that sensitive information, both in digital and physical format and assets (e.g., notebooks, cellphones, tablets, etc.) are not left unprotected at personal and public workspaces when they are not in use, or when someone leaves his/her workstation, either for a short time or at the end of the day.

Since information and assets at a workspace are in one of their most vulnerable places (subject to disclosure or unauthorized use, as mentioned under the Acceptable Usage Policy), the adoption of a Clear Desk and Clear Screen Policy is one of the top strategies to utilize when trying to reduce the risk of security breaches.

This Clear Desk/ Clear Screen Policy covers the purpose, scope, application, Policy ownership, and Policy.

11.1.1. Purpose

To improve the security and confidentiality of information, SDP shall adopt a Clear Desk Policy for papers and removable storage media and a Clear Screen Policy for information processing facilities. This reduces the risk of unauthorized access, modification or damage to information during and outside regular working hours or when areas are unattended.

11.1.2. Scope

This control applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties who have access to SDP systems.

11.1.3. Application

This Policy applies to all staff and stakeholders with access to the State Department for Planning systems and applications.

11.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer.

11.2. Policy

All staff shall be required to lock away all sensitive or critical business information when not required.

11.2.1. All staff shall not leave confidential information in the open while you are away from your desk

11.2.2. The Organization does not accept any responsibility for personal possessions. All personal possessions should be securely kept.

11.2.3. All staff shall ensure that pedestals, cupboards, and filing cabinets are locked.

11.2.4. Unauthorized use of photocopiers and other reproduction technology must be prevented

11.2.5. All information or media containing sensitive or classified information shall be removed from all the originator's printing devices immediately and kept away safely when not in use.

11.2.6. All staff shall activate the lock screen command to lock and secure the PC while leaving their work station either for a while or in the evening when going home.

11.2.7. All organization-supplied notebooks or mobile devices shall be locked away when not in use.

11.2.8. All users shall log out and switch off PCs' at the end of the day and ensure all electrical equipment is switched off at night and when appropriate.

11.2.9. Computers and terminals shall be left logged off or protected with screen and keyboard logging mechanism controlled by password, token or similar security solutions.

11.2.10. All staff shall not leave any documentation or media containing information belonging to SDP unattended.

11.2.11. Regular and ongoing Clear Desk, Clear Screen audits shall be undertaken to ensure continued employee compliance with this Policy.

12. Bring Your Own Device(BYOD)

12.1. Introduction

This Policy controls user-owned devices in the SDP's environment for access and processing of work-related information. The need for the use of Bring Your Own Device (BYOD) might be due to a shortage of devices or the interest/decision of staff to use a personal device while performing their day-to-day official roles and responsibilities. Users are not denied the use of the unique instrument, but they must abide by the guidelines outlined in this Policy.

What is BYOD?

Mobile computing is an increasing part of everyday life; as devices become smaller and more powerful, the number of tasks that can be achieved away from the office grows.

Mobile devices include items such as:

- Laptop and notebook computers
- Tablet devices
- Smartphones
- Personal Digital Assistants (PDAs)

Historically, the organization has provided the above devices where they are appropriate for exclusive business use. But the low cost and general availability of such devices have fueled the desire amongst employees and other stakeholders to use their own devices for business use.

In some cases, this can provide increased flexibility and remove the need for the employee to carry more than one device regularly. However, the concept of allowing an employee to make use of their instrument (s) for business purposes may result in the need for such devices to be subjected to additional controls over and above those typically in place for a personal device.

Common issues and security challenges with BYOD may include:

a) Use of the device by other family members.
b) Default storage of data in cloud backup facilities.
c) Increased exposure to potential loss in social situations, e.g., on the beach, in a bar.
d) Potential access to websites that do not meet the organization’s Acceptable Use Policy.
e) Connection to insecure networks, e.g., unsecured wireless hotspots.
f) Anti-virus protection and how often the device is patched.
g) Installation of potentially malicious apps onto the device (often without the user being aware that they are malicious).

These issues must be considered when assessing the suitability of any given device to hold specific data belonging to the organization.

This BYOD Policy covers the purpose, scope, application, Policy ownership, and the approach which addresses the use of one's equipment, BYOD assessment process, audit and monitoring, physical protection, access controls, cryptographic techniques, backup, virus protection, network connection, and overlooking.

12.1.1. Purpose

The purpose of this Policy is to set out the controls that must be in place when using mobile devices that are not owned or provided by the State Department for Planning. It is intended to mitigate the following general risks:

1) Loss or theft of mobile devices, including the data on them
2) Compromise of classified information through observation by the public
3) Introduction of viruses and malware to the network
4) Loss of reputation

The controls set out in this Policy must be observed at all times in the use and transport of BYOD mobile devices. It is a joint decision between the SDP and the device owner concerning whether any particular device shall be used for business purposes. Such use is not compulsory, and the employee has the right to decide whether the additional controls placed on the device by the SDP are acceptable and, therefore, whether they choose to use the machine for business purposes or use the usually provided devices.

12.1.2. Scope

This control applies to all systems, people, and processes that constitute the SDP's information systems, including board members, directors, employees, suppliers, and other third parties who have access to SDP's systems.

12.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

12.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the document Policy at regular intervals with the approval of the Accounting Officer.

12.2. Policy

12.2.1. BYOD (Use of One's Own Personal Equipment)

12.2.1.1. A user may use their equipment with prior administrative approval.

12.2.1.2. The user shall;

a) Be solely responsible for the security and other protection of such equipment and the data therein,
b) The user shall not hold the administration responsible for any loss or damage to their equipment while within the premises.

12.2.2. BYOD Assessment Process

12.2.2.1. Individuals shall not use their own devices to hold and process SDP's information unless they have submitted a request to do so and that request has been formally approved.

12.2.2.2. Assessment of each BYOD request on an individual basis to establish:

a) The identity of the person making the request
b) The business reason for the request
c) The data that shall be held or processed on the device
d) The specific device that shall be used

12.2.2.3. Requests shall be submitted to the IT service desk.

The general principle of this Policy is that the degree of control exercised by the SDP over the BYOD device shall be appropriate to the sensitivity of the data held on it. The Information Security document describes the Information Classification Scheme in use within the SDP.

12.2.3. Audit and Monitoring

To ensure SDP data is adequately protected, the IT Department shall monitor and audit the level of compliance with this Policy. The story of monitoring and audit shall be appropriate to the classification of the information held on the device.

12.2.4. BYOD Conditions of Use

As a BYOD mobile device user, you agree to comply with the following conditions of use.

12.2.5. Physical Protection

12.2.5.1. All staff shall ensure that the device is transported in a protective case when possible and is not exposed to situations that may become damaged.

12.2.5.2. Devices shall not be left unattended in public view, such as in the back of a car, meeting room, or hotel lobby.

12.2.5.3. All staff shall ensure that the device is locked away when being stored and that the key is not easily accessible.

12.2.6. Access Controls

12.2.6.1. All staff shall not hold classified information on the device unless authorized and appropriate controls (e.g., encryption) are implemented.

12.2.6.2. All staff shall not keep access tokens, Personal Identification Numbers, or other security items with the device.

12.2.6.3. All staff shall ensure that the device screen locks after a short period of not being used and requires an access code or password to unlock it.

12.2.6.4. Passwords used shall be solid and challenging to guess.

12.2.6.5. No unsecured logins (i.e., those that do not require a password) that access classified information should be set up on the device.

12.2.6.6. You shall not attempt to “jailbreak” the device so that the supplier’s security controls are disabled.

12.2.6.7. You may be asked to return the device to the IT Service Desk at any time for inspection and audit.

12.2.7. Cryptographic Techniques

12.2.7.1. Where possible, devices shall be secured so that all of the data is encrypted and is only accessible if the password is known.

12.2.7.2. If the device is supplied with encryption already turned on, do not disable it.

12.2.8. Backups

12.2.8.1. Changes to files held locally on the device shall be backed up regularly.

12.2.8.2. Corporate data should be backed up to the corporate network when possible.

12.2.8.3. Staff are discouraged from taking unencrypted backups of classified information, e.g., to a cloud storage provider.

12.2.9. Virus Protection

12.2.9.1. The BYOD device shall be installed with an updated endpoint protection system.

12.2.9.2. Do not disable virus protection on the device.

12.2.9.3. Staff shall only purchase and install apps from a reputable source

12.2.10. Network Connection

Staff should be wary of automatically connecting to wireless networks or open networks in public places, e.g., airports.

12.2.11. Overlooking

When in public places, staff shall ensure that the device is positioned in such a manner that unauthorized people cannot view (or take photographs or video of) the screen.

13. Identity and Access Management

13.1. Introduction

This Policy aims to provide guidelines for logical access control to the State Department for Planning systems and networks.

The control of access to our information assets is a fundamental part of an in-depth defense strategy to Information Security. If we are to effectively protect the confidentiality, integrity, and availability of classified data, we must ensure that a comprehensive mix of physical and logical controls is in place.

The Policy concerning access control must ensure that the measures implemented are appropriate to the State Department's requirement for protection and are not unnecessarily strict. Therefore, the approach must be based upon a clear understanding of the business requirements as specified by the owners of the assets involved.

This Identity and Access Management Policy provides guidelines and procedures to govern the use of equipment and technologies and help ensure effective network and systems management. Directorates, Departments, Sections and Units may adopt additional rules and regulations to meet specific administrative or business needs. Any adopted requirements must comply with this Policy.

13.1.1. Purpose

This Policy covers the purpose, scope, application, Policy ownership, and the approach which addresses requirements for access control, user access management, user registration and deregistration, user access provisioning, removal or adjustment of access rights, management of privileged access rights, user authentication for external connections, third party remote access to the organization network, and review of user access rights.

13.1.2. Scope

This control applies to all systems, people, and processes that constitute the organization's information systems, including staff and other third parties who have access to the State Department for Planning strategies.

Authority for exemption or non-compliance can be granted by the Accounting Officer in case of any network security concerns.

13.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

13.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has the ultimate responsibility for reviewing the Policy at regular intervals with the approval of the Accounting Officer.

13.2. Policy

The Policy covers the requirements for access control, user access management, user registration and deregistration, user access provisioning, removal or adjustment of access rights, management of privileged access rights, user authentication for external connections, Third-party remote access to the Organization Network, and Review of User Access Rights.

13.2.1. Requirements for Access Control

Requirements for access control may depend on factors such as:

a) The security classification of the information stored and processed by a particular system or service
b) Relevant legislation that may apply, such as the Data Protection Act, Kenya National Archives and Documentation Services (KNADS) Act, Access Information Act, among others
c) The regulatory framework in which the organization and the system operates
d) Contractual obligations to external third parties
e) The threats, vulnerabilities, and risks involved
f) The State Department's appetite for risk

13.2.2. User Access Management

13.2.2.1. Formal user access control procedures must be documented, implemented, and kept up to date for each application and information system. The documentation must cover all stages of the user access life cycle, from the initial registration of new users to the final deregistration of users who no longer require access.

13.2.2.2. User access rights must be reviewed regularly to ensure that the appropriate rights are still allocated.

13.2.2.3. System administration accounts must only be provided to users required to perform system administration tasks.

13.2.2.4. Separate system administration user credentials shall be defined for different users authorized to have administrative rights to systems. Administration user accounts credentials must not be shared to ensure non-repudiation.

13.2.3. User Registration and Deregistration

13.2.3.1. A request for access to the State Department's network and computer systems must be submitted to the appropriate system owner for approval. A user account for new staff members, temporary staff members, and guests shall only be set up based on the system managers' receipt of written authorization from either the new user's manager or the Human Resources Department

13.2.3.2. All requests shall be processed according to a formal procedure that ensures appropriate security checks are carried out and correct authorization is obtained before user account creation.

13.2.3.3. The principle of segregation of duties shall apply so that different people perform the creation of user accounts and the assignment of permissions.

13.2.3.4. Each user account shall have a unique user name that is not shared with any other user and is associated with a specific individual, not a role or job title. Generic user accounts that are to be used by a group of people should not be created as they provide an insufficient allocation of responsibility.

13.2.3.5. An initial strong password should be created on account setup and communicated to the user via secure means. The user must change the password on the first use of the account.

13.2.3.6. The Human Resource Department must notify the system manager or owner when staff members have left the State Department to facilitate revocation of user access rights.

13.2.3.7. When an employee leaves the State Department under normal circumstances, their access to networks, computer systems, and data must be suspended at the close of business on the employee's last working day. It is the supervisor's responsibility to request the suspension of the access rights via the authorized system owner.

13.2.3.8. In exceptional circumstances where there is perceived risk that the employee may take action that may harm the organization before or upon termination, a request to remove access may be approved, and actioned in advance of notice of termination is given.

13.2.3.9. User accounts should be initially suspended or disabled only and not deleted. User account names should not be reused as this may confuse the event of a later investigation.

13.2.4. User Access Provisioning

13.2.4.1. Each user must be allocated access rights and permissions to networks, computer systems, and data commensurate with their routine tasks.

13.2.4.2. Group roles should be maintained in line with business requirements, and any changes to them should be formally authorized and controlled via a change management process.

13.2.4.3. Ad-hoc additional permissions should not be granted to user accounts outside of the group role. If such approvals are required, this should be addressed as a change and formally requested.

13.2.5. Removal or Adjustment of Access Rights

13.2.5.1. An adjustment of access rights or permissions is required; for example, due to a role change or a newly assigned role, the difference in access rights should be authorized through a change management process as soon as the new position is set.

13.2.5.2. Due consideration of any issues of segregation of duties should be given.

13.2.5.3. Under no circumstances should administrators be permitted to change their user accounts or permissions.

13.2.6. Management of Privileged Access Rights

13.2.6.1. Privileged access rights associated with administrator-level accounts must be identified for each system or network and tightly controlled.

13.2.6.2. Technical system users (such as IT staff) should not make day-to-day use of user accounts with privileged access. Instead, a separate administrator-level user account should be created and used only when additional privileges are required.

13.2.6.3. Administrator-level accounts should be specific to an individual, e.g., "John Smith Admin"; generic administrator-level accounts should not be used as they provide insufficient user identification.

13.2.6.4. Access to administrator-level permissions should only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.

13.2.6.5. The use of user accounts with privileged access in automated routine tasks should be avoided where possible. Where this is unavoidable, the password used should be protected and changed regularly.

13.2.7. User Authentication for External Connections

13.2.7.1. In line with the Network Security Policy, the use of modems on non-organization-owned computing devices connected to the organization's network can seriously compromise the network's security. Specific approval must be obtained from the officer charged with the responsibility for Information Security before connecting any equipment to the organization's network.

13.2.7.2. Where remote access to the network is required via VPN, a request must be through the officer responsible for Information Security.

13.2.7.3. A Policy for using two-factor authentication for remote access should be used in line with the principle of “something you have and something you know" where applicable, to reduce the risk of unauthorized access from the Internet.

13.2.8. Third-Party Remote Access to the Organization Network

13.2.8.1. Partner agencies or 3rd parties must not be given details of how to access the organization's network without permission from the Accounting Officer.

13.2.8.2. Any changes to third-party connections (e.g., on termination of a contract) must be immediately sent to the person charged with managing the system.

13.2.8.3. Partners or 3rd party suppliers must contact the person charged with managing the system on each occasion to request permission to connect to the network. A log of activity must be maintained.

13.2.8.4. Remote access software and user accounts must be disabled when not in use.

13.2.9. Review of User Access Rights

13.2.9.1. Regularly (at least annually), asset and system owners shall be required to review who has access to their areas of responsibility and the level of access in place. This shall be to identify:

a) People who should not have access.
b) User accounts with more access than required by the role.
c) User accounts with incorrect role allocations.
d) User accounts that do not provide adequate identification, e.g., generic or shared accounts.
e) Any other issues that do not comply with this or different relevant Policy.

13.2.9.2. This review shall be performed according to a formal procedure and any corrective actions identified and carried out.

13.2.9.3. The person charged with managing Information Security every quarter conduct a review of user accounts with privileged access.

14. Password Management

14.1. Introduction

Passwords are an essential aspect of Information Security. They provide authorized users with a means to access networks and information systems. Poor management of passwords can comprise the confidentiality, integrity, and availability of systems accessed within or managed by the State Department. Therefore, it is imperative that the State Department employees and any appropriate third parties authorized to access methods take proper steps to secure their passwords. System owners and the ICT Unit should also ensure that passwords are appropriately managed within the State Department.

This Password Management Policy covers the purpose, scope, application, Policy ownership, and procedure.

14.1.1. Purpose

This Policy aims to provide guidelines for user authentication and access control using passwords in the State Department for Planning.

The State Department's network and systems are owned by the Government of Kenya and are provided to support the business processes and functions of the Government. Adherence to the Policy shall help protect the integrity of the Government network and systems and the information and data stored and transmitted. Enforcement actions shall mitigate risks and losses associated with security threats to the network and systems. This Policy provides guidelines and procedures to govern password management for access to systems and networks. Directorates/Departments/Sections/Units may adopt additional rules and regulations to meet specific administrative or business needs. Any adopted requirements must comply with this Policy.

14.1.2. Scope

This control applies to all systems, people, and processes that constitute the organization's information systems, including staff and other third parties who have access to the State Department for Planning systems and applications.

Authority for exemption or non-compliance can be granted by the Authorized/Accounting Officer in case of any network security concerns.

14.1.3. Application

This Policy applies to all staff and stakeholders with access to the State Department for Planning systems and applications.

14.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has ultimate responsibility for reviewing the document Policy at regular intervals with the approval of the Accounting Officer.

14.2. Policy

14.2.1. All State Department’s networks and systems, including computing devices, shall be accessed using appropriate credentials, which involve but are not limited to user names and passwords.

14.2.2. The State Department’s Policy may make use of additional authentication methods based on a risk assessment which takes into account:

a) The value of the assets protected.
b) The degree of threat believed to exist.
c) The cost of the additional authentication method(s).
d) The ease of use and practicality of the proposed method(s).
e) Any other relevant controls in place.

14.2.3. Multi-factor authentication methods should be justified based on the above factors and securely implemented and maintained where appropriate.

14.2.4. Single Sign-On (SSO) shall be used within the internal network where relevant systems support them unless the security requirements are deemed to be such that a further login is required.

14.2.5. Whether single or multi-factor authentication is used, the quality of user passwords should be enforced in all networks and systems using the following parameters:

a) Be at least 8 characters in length.
b) Contain both upper and lowercase alphabetic characters (e.g., A-Z, a-z).
c) Have at least one numerical character (e.g., 0-9).
d) Have at least one unique character (e.g., ~!@#$%^&*()_-+=).
e) A Strong Password should not:-
f) Spell a word or series of words that can be found in a standard dictionary.
g) Spell a word with a number added to the beginning and the end.
h) Be based on personal information such as user id, family name, pet, birthday, etc.

The following are recommendations for maintaining a Strong Password:

14.2.6. Passwords should not be shared with anyone for any reason. When someone requires access to another individual's protected resources, the delegation of permission options should be explored. Passwords should not be shared even for computer repair— an alternative should be explored by creating a new account with an appropriate level of access for the repair person.

14.2.7. Passwords should be changed upon indication of compromise. If one suspect's that someone has compromised their account, they should change their password immediately.

14.2.8. Passwords should not be written down or stored in an insecure manner. In cases where it is necessary to write down a password, that password should be stored in a secure location and adequately destroyed when no longer needed.

14.2.9. The password manager should not be used to store passwords unless the password manager leverages strong encryption and requires authentication before use.

14.2.10. Users shall avoid reusing passwords. When changing an account password, users should avoid reusing previous passwords.

14.2.11. Users should avoid using the same password for multiple accounts.

14.2.12. Automatic login functionality for systems should be disabled.

14.2.13. Where applicable, the system shall force the expiration of passwords after a specified period.

14.2.14. The user's identity shall be verified before resetting a password.

14.2.15. Default account passwords and vendor default passwords must be changed immediately upon installation and configuration of the system or application.

14.2.16. Passwords should not be stored or transmitted without encryption or using weak encryption or hashing algorithms.

14.2.17. Automated notification of a password changes or reset shall be implemented.

14.2.18. Users shall be notified through official emails of any changes to their credentials. This provides a user with a confirmation that the change or reset was successful and alerts a user if their password was unknowingly changed or reset.

14.2.19. User accounts should be locked after 5 failed login attempts whenever possible. Once locked out, the user account shall remain closed for a specified period unless manually unlocked.

14.2.20. When leaving a workstation, a staff member shall log out of all systems and networks adequately. Resumption of access shall require the user’s password.

14.2.21. Systems and networks should maintain access logs to facilitate access investigation when necessary. System access logs shall be kept for a specified period.

15. Network Access

15.1. Introduction

The purpose of this Policy is to provide guidelines for access to the network infrastructure and devices managed, controlled, or within the jurisdiction of the State Department for Planning.

This Network Access Policy covers the purpose, scope, application, Policy ownership, and the approach which addresses remote access, wireless communication, Virtual Private Networks (VPNs), and network access controls.

15.1.1. Purpose

The purpose of this Policy is to establish management's criteria for accessing the State Department for Planning network infrastructure and systems to forestall uncontrolled or unauthorized access that may result in security breaches or the misuse of corporate resources.

15.1.2. Scope

The scope of this Policy extends to all network resources involved in the transmission of the State Department's information.

Authority for exemption or non-compliance can be granted by the Accounting Officer in case of any network security concerns.

15.1.3. Application

The Policy applies to all employees and third parties and permits access to the State Departments' network and network resources.

15.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer.

15.2. Policy

The Policy covers remote access, dial-in access, wireless communication, Virtual Private Networks (VPNs) and network access controls.

15.2.1. Remote Access

15.2.1.1. Remote access must be strictly controlled, with required approval.

15.2.1.2. No time shall any of the State Department's remote users release their login details to anyone.

15.2.1.3. Employees and third parties must ensure that their personal computers or workstations are not connected to the State Department's corporate network and any other external network in line with the Network Policy.

15.2.1.4. All hosts connected to the State Department’s internal networks via remote access technologies, including personal computers, must use the most up-to-date anti-virus and operating systems.

15.2.1.5. Third-party connections must comply with requirements as stated in the Network Policy.

15.2.1.6. Personal equipment used to connect to the State Department’s networks must comply with this Policy and the Network Policy.

15.2.2. Dial-In and Remote Access

15.2.2.1. Remote access must be granted and managed in line with the Network Policy.

15.2.2.2. The State Department's employees and approved authorized third parties (consultants, vendors, etc.) may use remote connections to access the corporate network where necessary.

15.2.2.3. Remote access must be strictly controlled and granted based on business justification.

15.2.2.4. A user who is granted remote access or dial-in access privileges must constantly be made aware that connections between their location and the State Department are literal extensions of its corporate network. The employee and approved authorized third party individual must take every reasonable measure to protect the State Department's assets.

15.2.2.5. Users with remote access privileges must ensure that unauthorized persons do not use remote access or dial-in connection to the State Department to gain access to the State Department's information system resources.

15.2.2.6. Users shall be held accountable where their remote access credentials are used to compromise or breach the State Department’s network.

15.2.2.7. Activity on dial-in accounts must be monitored, and access, as well as activity logs, maintained. Remote access and dial-in connections must log out fifteen (15) minutes of inactivity.

15.2.2.8. Remote access and dial-in connections user credentials not used for a specified period must be disabled. If access is subsequently required, the individual must request a re-activation or a new account.

15.2.3. Wireless Communication

15.2.3.1. Wireless communication, connectivity, and access shall be managed according to the Network Policy.

15.2.3.2. The Head of ICT must approve all wireless access points and routers connected to the corporate network after concurrence with the Department responsible for managing the Government Network, GCCN.

15.2.3.3. Periodic penetration and vulnerability tests and audits must be carried out on all wireless access points and routers.

15.2.3.4. All wireless Network Interface Cards, modems, and wireless USB adapters used in corporate laptop or desktop computers must be registered with the ICT Unit.

15.2.3.5. All wireless (Local Area Network - LAN) access must use products from approved vendors.

15.2.3.6. Approved security configurations must be documented and implemented on all wireless access points and routers in collaboration with the Department responsible for managing the Government Network, GCCN.

15.2.3.7. All implementations must support and employ appropriate user authentication according to the Access and Password Policies.

15.2.3.8. Base stations or wireless routers must be configured so that the name does not contain any identifying information about the State Department, such as the Organization's/Department's name, division title, employee name, or product identifier.

15.2.4. Virtual Private Networks (VPNs)

15.2.4.1. It is the responsibility of users with VPN privileges to ensure that unauthorized people are not allowed access to the State Department's internal networks.

15.2.4.2. Dual (split) tunneling is not permitted; only one network connection should be allowed following the Network Policy where applicable.

15.2.4.3. Every configuration change must go through testing duly and should be approved by the Department in charge of managing the Government Network where applicable, the person responsible for Information Security and the Head of ICT.

15.2.4.4. All computers connected to the State Department's internal networks via VPN or other technology must use the most up-to-date anti-virus and operating system.

15.2.4.5. VPN users must be automatically disconnected from the State Department's network after fifteen (15) minutes of inactivity.

15.2.4.6. The VPN concentrator must be limited to an absolute connection time of 3 hours.

15.2.4.7. Personal computers/equipment used on the State Department's VPN must be configured to comply with the network access, password, and network policies.

15.2.4.8. Only VPN clients approved in line with the Network Policy shall be used.

15.2.4.9. Users shall execute a non-disclosure agreement and VPN declaration before access is granted.

15.2.4.10. The Accounting Officer should approve the business justification for VPN access.

15.2.4.11. Using VPN technology with personal equipment makes users understand that their machines are a de-facto extension of the State Department's network. As such are subject to the same rules and regulations that apply to the State Department-owned equipment, i.e., their machines must be configured to comply with the State Department's Information Security Policies.

15.2.5. Network Access Controls

15.2.5.1. Access to the State Department's network should be granted only to authorized users (On a "need to have" basis).

15.2.5.2. Secure protocols must be used for accessing all services that require authentication. These should be documented with business justification.

15.2.5.3. The use of open ports and unused services on servers and network devices without business need/justification is not allowed.

15.2.5.4. All security breaches must be reported to the officer charged with Information Security and designated authorities.

15.2.5.5. Security warning/notification must be displayed before allowing log-on on systems running applications accessible on the State Department's network.

15.2.5.6. At no one time should a third-party system be connected to the State Department's network without prior authorization from designated authorities.

15.2.5.7. Network access control solution should be implemented to address host integrity checks on systems before access is granted into the State Department's network.

15.2.5.8. Periodic (quarterly) vulnerability assessment and reporting must be performed by the State Department’s authorized subject matter expert to help manage system security needs.

15.2.5.9. The ICT Unit should check third-party systems to ensure no threats /viruses and meet minimum security configuration requirements.

16. Personnel and Awareness

16.1. Introduction

State Department for Planning encourages all employees associated to continuously exert their professionalism and efforts in discharging their responsibilities towards enhancing service delivery. The purpose of this Policy is to ensure that SDP inculcates Information Security in human resource management and to do so with due regard for the complexities of Public Service operations, the individuality of each of its staff members and in line with the Human Resource Policies and Procedures Manual (HRPPM).

The Human Resource Policies and Procedures Manual set out the conditions of service, duties, and obligations of staff members, appointments, and termination procedures.

This Personnel Awareness Policy covers the purpose, scope, application, Policy ownership, and the Policy, which addresses rights and responsibilities of employer and employee covering before employment, during employment, and termination or change of employment.

16.1.1. Purpose

The purpose of this Policy is to ensure that employees understand their responsibilities and are suitable for the roles for which they are considered. During employment, the Policy ensures that employees are aware of and fulfill their Information Security responsibilities. At termination or change in work, it ensures that Government's interests are protected.

16.1.2. Scope

This Policy applies to all personnel with access to Government services and systems regarding the following areas:

1) Before employment.
2) During employment.
3) Termination or Change of Employment.

16.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

16.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer and in collaboration with the Department in charge of Human Resources.

16.2. Policy

The Policy covers the rights and responsibilities of the employer and employee, before employment, during employment and termination or change of employment.

16.2.1. Rights and Responsibilities of the employer and employee

In the State Department for Planning, personnel policies and procedures aim to bring harmony in the work environment. They are also meant to promote effective communication among the appraisee and supervisor and protect and clarify the rights and responsibilities of both the employer and employees. They are as outlined below;

16.2.1.1. The State Department shall implement and maintain a comprehensive set of Information Security controls concerning personnel that meet requirements identified by a risk assessment.

16.2.1.2. The State Department shall use sections relevant policies to identify possible Information Security risks and procedures to treat identified risks associated with personnel.

16.2.1.3. The State Department shall consider legislation and Policy that governs employment and conditions of personnel in line with the Human Resource Policies and Procedures Manual. This shall include legislation, Policy, and contracts that govern employees and other stakeholders who access the State Department's information resources.

16.2.2. Before employment

To ensure that employees understand their responsibilities and are suitable for the roles for which they are considered as outlined below;

16.2.2.1. Background verification checks on all candidates for employment following relevant laws, regulations, and ethics shall be carried out.

16.2.2.2. Accounting Officers shall ensure that all newly appointed officers are duly vetted per the existing Vetting Policy.

16.2.2.3. The basis of verification shall be the classification of information to be accessed and perceived risk.

16.2.2.4. The candidate shall, on the first appointment, provide the document as specified in the HRPPM

16.2.2.5. A candidate with a record of conviction shall be employed only with the concurrence of the Public Service Commission.

16.2.2.6. A candidate whose appointment in the Public Service had been terminated for any reason, including resignation, shall not be employed without prior approval of the Public Service Commission.

16.2.2.7. All applicable laws and regulations must secure information gathered on potential employees. Access must be limited to a 'need to know basis.

16.2.3. During employment

To ensure that employees are aware of and fulfill their Information Security responsibilities as outlined below:

16.2.3.1. All employees are required to apply Information Security following the established policies and procedures of the organization.

16.2.3.2. All new employees shall be inducted on Information Security.

16.2.3.3. All employees shall conform to the terms and conditions of employment.

16.2.3.4. Employees must be adequately briefed on their Information Security roles and responsibilities before being granted access to information systems.

16.2.3.5. Employees shall be provided with guidelines to state Information Security expectations of their roles within the State Department.

16.2.3.6. Employees shall be provided with an anonymous reporting channel to report a violation of Information Security policies or procedures.

16.2.3.7. Employees shall sign an appropriate confidentiality agreement at the time of appointment.

16.2.3.8. All employees of the SDP shall receive regular updates on the State Department policies and procedures as relevant for their job function.

16.2.3.9. A public officer shall ensure that confidential or secret information or documents entrusted to their care are adequately protected from improper or inadvertent disclosure.

16.2.3.10. The information shall be availed to employees on the need-to-know principle to access information for their assigned duties.

16.2.3.11. Regulations governing discipline in the Public Service and the procedure shall be enforced in cases of breach of discipline as contained in the Public Service Commission Regulations.

16.2.3.12. Employees shall comply with Chapter Six of the Constitution on Leadership and Integrity in line with the HRPPM.

16.2.3.13. Officers shall adhere to their professional code of conduct.

16.2.4. Termination or Change of Employment

To protect the interest of the SDP as part of changing or terminating employment. It shall seek to ensure that Information Security is not compromised during this process.

16.2.4.1. Duties and responsibilities of the employees who have been disengaged or transferred shall be delegated or allocated to another employee.

16.2.4.2. Changes of responsibility or employment shall be managed as the termination of the respective responsibility or jobs.

16.2.4.3. Responsibilities and duties that remain valid after termination or employment change shall be defined, communicated to the employee, and enforced.

16.2.4.4. All the personnel and operating arrangements changes shall be communicated to the employees when necessary.

16.2.4.5. All employees shall return all the assets they are responsible for upon termination of their employment, contract, or agreement.

16.2.4.6. An Accounting Officer may terminate the employment of an officer serving on a contract or probationary terms following the provisions of the officer's agreement.

16.2.4.7. Upon termination, an individual's access rights to assets associated with information systems and services shall be reconsidered.

17. Incident Management

17.1. Introduction

This section provides a Policy for managing incidents within the State Department. An Information Security incident is an identified occurrence of a system, service, or network state indicating a possible breach of Information Security Policy or failure of safeguards or a previously unknown situation that may be Information Security-relevant.

This Incident Management Policy covers the purpose, scope, application, Policy ownership, and the approach which addresses incident management controls and planning for Information Security incidents.

17.1.1. Purpose

To define the response plan to an Information Security incident as indicated by a single or series of unwanted or unexpected Information Security events that have a significant probability of compromising business operations or threatening Information Security.

17.1.2. Scope

This Policy applies to the entire incident management process, including detection, assessment, containment, recovery, and post mortem.

17.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

17.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has ultimate responsibility for reviewing the document Policy at regular intervals with the approval of the Accounting Officer.

17.2. Policy

The Policy covers incident management controls and Planning for Information Security Incidents

17.2.1. Incident Management Controls

Incident Management Controls include all activities that ensure a consistent and effective approach is applied to managing Information Security incidents. The SDP shall;

17.2.1.1. Implement and maintain incident management controls that meet requirements identified by a risk assessment.

17.2.1.2. Establish Information Security incident management procedures to ensure appropriate responses in Information Security incidents, breaches, or system failures.

17.2.1.3. Establish and maintain an Information Security incident register and record all incidents.

17.2.1.4. Ensure all Information Security incidents are reported and escalated (where applicable) through appropriate management channels and authorities.

17.2.1.5. Investigate deliberate violation or breach of this Information Security Policy or subordinate processes on occurrence, and institute formal disciplinary procedures.

17.2.1.6. Ensure responsibilities and procedures for the timely reporting of security events and incidents, including breaches, threats, and security weaknesses, are communicated to all employees, including contractors and third parties.

17.2.1.7. Liaise with relevant authorities at the earliest opportunity when criminal activity affecting Information Security is identified.

17.2.1.8. Ensure the relevant Government of Kenya ICT Standards for guidance on managing Information Security incidents are made.

17.2.1.9. Evaluate a decision to invoke legal action that may alter the priorities and procedures that are to be followed. For example, retention of evidence in a form to support a police investigation and possible prosecution may delay the resolution of any incident or delay the implementation of any preventative measures.

17.2.1.10. It is recommended that agencies implement procedures to determine if and when legal action is to be pursued, including:

a) Internal processes to approve referral to the investigative agencies;
b) Rules to assist in determining when incidents shall be referred to the investigative agencies; and
c) Regulations and procedures to ensure that evidence is retained in a form suitable for investigation and prosecution.

17.2.2. Planning for Information Security Incidents

17.2.2.1. The Security Incident Management Plan should include general priorities for action during an incident. The preferences may change depending on the nature of the incident. Recommended priorities are:

a) Protection of human life and people’s safety,
b) Security of sensitive information,
c) Security of other information,
d) The decision to pursue legal action,
e) Prevention of irreparable damage to systems,
f) Internal and external communication of the incident, and
g) Minimizing disruption to services.

17.2.2.2. SDP shall establish roles and responsibilities to ensure that incident responses are appropriately managed. It is recommended that contact lists of the following are prepared:

a) State Departments staff responsible for each site;
b) External property managers (for leased areas);
c) State Departments business owners of systems and sites;
d) ICT system managers, including appropriate contracted suppliers;

e) SDP/Government media liaison staff;
f) SDP senior managers; and
g) Police contacts to be used if legal action is to be pursued.

17.2.2.3. If an Information Security incident that affects the general public occurs, it is recommended that SDP liaise with media Units to establish appropriate public communication procedures. In doing so, they may consider:

a) The visibility and impact of such an incident on staff,
b) The visibility and impact of such incidents on services with other agencies and the public,
c) Potential media interest in the incident, and
d) The possible political implications of the incident.

18. Change Management

18.1. Introduction

This section provides a Policy for facilitating change management within the State Department. Newly introduced systems or changes to existing systems can be highly disruptive to operations in an organization. However, well-executed change management initiatives ensure smooth transitions to new work processes, thus eliminating interruptions to organization operations.

This Change Management Policy covers the purpose, scope, application, Policy ownership, and procedure.

18.1.1. Purpose

The purpose of this Policy is to guide SDP in instituting and undertaking change management to ensure that changes are carried out in a planned manner to minimize negative impact to services and customers.

18.1.2. Scope

This Policy covers all changes in implementing new ICT infrastructure, systems, and related technologies.

18.1.3. Application

This Policy applies to all users, technical staff, service providers, management, and other key stakeholders affected by the changes.

18.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has ultimate responsibility for reviewing the document Policy at regular intervals with the approval of the Accounting Officer.

18.2. Policy

Changes to configurations, systems, applications, or equipment that affect the work of more than one person shall follow the appropriate ICT change management procedures to minimize adverse impacts of the changes to operations.

18.2.1. All changes shall be initiated using a change request (RFC) form submitted by process owners and approved by respective HOD/HOC. RFC form shall contain enough information to enable evaluation of the potential impacts, risks, and benefits.

18.2.2. SDP change management procedure shall include:

a) Change classification based on the need and urgency.

b) Change evaluation considering the feasibility, human and physical resource requirements and costs, impact on service delivery, Information Security, and risks.

c) Notification on the time, duration, and potentially affected services should be sent to all customers affected by the change.

d) A roll-back plan that shall be developed and implemented before the change occurs.

18.2.3. Changes shall be tested in a test environment before implementation.

18.2.4. The change shall be effected at a time that shall minimize disruption to service delivery.

18.2.5. Users shall be notified of the change results once the changes are complete.

18.2.6. Users shall be taken through formal training on the new operational processes impacted by the change.

18.2.7. Users shall review and accept the changes and readiness for use and the review shall be documented.

18.2.8. The ICT Unit shall approve any equipment installation or removal and document.

19. Business Continuity Management

19.1. Introduction

This section provides a Policy for ensuring business continuity within the State Department. Business Continuity includes all activities that counteract interruptions to business activities to protect critical business processes and information from the effect of interruptions due to failures of ICT systems or disasters and to ensure their timely resumption.

This Business Continuity Management Policy covers the purpose, scope, application, Policy ownership, and procedure.

19.1.1. Purpose

To proactively plan, avoid, and mitigate risks associated with a disruption of operations. It details steps to be taken before, during, and after an event to maintain the organization's functions.

19.1.2. Scope

It details steps to be taken before, during, and after an event to maintain the operations of the SDP.

19.1.3. Application

This Policy applies to all staff and stakeholders with access to SDP systems and applications.

19.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer.

19.2. Policy

The State Department for Planning shall:

19.2.1. Implement and maintain business continuity management controls that meet the requirements identified by a risk assessment.

19.2.2. Develop methods to reduce known risks to information and ICT assets, including a business impact analysis.

19.2.3. Maintain and test business continuity plans to ensure information and ICT assets are available and consistent with the SDP business and mandate.

19.2.4. Ensure all critical business processes, associated information, and ICT assets are identified and prioritized.

19.2.5. Ensure compliance with the relevant Government of Kenya ICT Standards for guidance on managing business continuity.

20. ICT Disaster Recovery

20.1. Introduction

This section provides a Policy for facilitating ICT Disaster Recovery within the State Department. ICT Disaster Recovery includes all activities related to ensuring the availability of ICT systems and services, including restoring ICT systems and services following an event that disrupts service delivery or the continued operation.

This ICT Disaster Recovery Policy covers the purpose, scope, application, Policy ownership, and procedure.

20.1.1. Purpose

ICT Disaster Recovery supports business continuity activities but is distinct in focusing on the restoration of ICT services rather than on the restoration of business services themselves

20.1.2. Scope

Focuses on the critical ICT resources of the State Department for Planning.

20.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

20.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer.

20.2. Policy

The State Department for Planning shall;

20.2.1. Establish an ICT disaster recovery register to assess and classify ICT assets to determine their criticality.

20.2.2. Establish and maintain a register with details of suppliers of critical systems.

20.2.3. Establish plans and processes to assess the risk and impact of the loss of information and ICT assets in the event of a security failure or disaster to enable information and ICT assets to be restored or recovered.

20.2.4. Develop ICT Disaster Recovery Plans with clearly defined maximum acceptable downtimes.

20.2.5. Ensure the ICT disaster recovery plans are maintained and tested to ensure information and ICT assets are available and consistent with SDP business and service delivery requirements.

20.2.6. Define maximum acceptable downtimes for ICT services

20.2.7. Define service and operational level agreements with external parties where applicable.

20.2.8. Ensure copies of ICT disaster recovery plans are stored in multiple locations, including at least one location offsite.

21. Malware Management

21.2. Introduction

This section provides a Policy for malware management within the State Department. The number of computer security incidents caused by malware and viruses and the consequent cost of business interruption and service restoration continues to escalate. Implementing anti-malware and antivirus systems must reduce risks and manage the SDP computing environment.

This Malware Management Policy covers the purpose, scope, application, Policy ownership, and procedure.

21.2.1. Purpose

This Malware Management Control aims to enhance the security of end-user and computing devices to achieve business continuity.

21.2.2. Scope

This covers all forms of malware such as viruses, rootkits, worms, and trojans that can cause disruption/corrupt the systems and applications.

21.2.3. Application

This Policy applies to all staff and stakeholders with access to the State Department for Planning systems and applications.

21.2.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has ultimate responsibility for reviewing the Policy document at regular intervals with the approval of the Accounting Officer.

21.3. Policy

21.3.1. The ICT Unit shall ensure that approved and maintained licensed antivirus and Anti Malware software from known and trusted sources is deployed.

21.3.2. All SDP computers and computing devices shall run on the SDP approved, updated, and licensed anti-malware software.

21.3.3. Users shall regularly initiate the scan and update the software to protect against the latest threats.

21.3.4. All SDP-issued computers must use the antivirus software installed and configured by the ICT Unit.

21.3.5. Users are prohibited from disabling or tampering with the installed antivirus software.

21.3.6. When a computer system is determined to be infected with a virus or other malicious software, that system may be blocked and removed from the network until the threat is neutralized.

21.3.7. In an attack beyond SDP’s control, the Department shall seek technical assistance from relevant Government agencies.

22. Use of Cloud Services

22.1. Introduction

This section provides a Policy for guiding the use of cloud and private hosting services by the State Department. Cloud computing offers an alternative model for delivering ICT services. It allows individuals and organizations to use software, hardware, and services hosted separately from the Governments' facilities and managed by Private Sector organizations. Care must be taken to mitigate risks associated with using cloud services.

Adopting this model shall require:

a) Due diligence and prudence when selecting an appropriate Cloud Service Provider (CSP)
b) A clear delineation of the roles and responsibilities between the State Department and the CSP for implementing, operating, and maintaining security controls that support the State Department's obligations for data protection and privacy as well as safeguarding the confidentiality, integrity, and availability of data, information, and IT assets

This Policy on the use of cloud services covers the purpose, scope, application, Policy ownership, and procedure.

22.1.1. Purpose

The purpose of this Policy is to set out guidance to assist the State Department in the safe use of private or commercial cloud services.

22.1.2. Scope

This Policy covers all cloud services, including private or commercial hosting services.

22.1.3. Application

This Policy applies to all staff and stakeholders with access to State Department for Planning systems and applications.

22.1.4. Policy Ownership

The person charged with the responsibility for Information Security is the owner of this document and has ultimate responsibility for reviewing the document Policy at regular intervals with the approval of the Accounting Officer.

22.2. Policy

22.2.1. The use of cloud computing services must comply with all current laws and regulations of the Government of Kenya.

22.2.2. Departments shall not host critical applications in the public cloud or private hosting providers without consultation of the Ministry of ICT, the ICT Unit, and express approval of the Accounting Officer.

22.2.3. Cloud services and private hosting services shall only be considered after a thorough risk evaluation has been completed, reviewed, and accepted by the person in charge of Information Security in the State Department.

22.2.4. To mitigate against risks associated with vendor lock-in, the State Department shall prepare an exit strategy as part of contracting with the Cloud Service Provider. The State Department shall also ensure that the Cloud Service Provider provides a mechanism to facilitate the movement of data, information, systems, and applications between multiple cloud service providers at low cost and minimal disruption.

22.2.5. The State Department shall obtain security assessment/assurance as early in the procurement cycle as possible for potential cloud service providers.

22.2.6. Cloud solutions that store personally identifiable citizen data shall be within the boundaries of Kenya.

22.2.7. The State Department shall ensure the protection, assurance, proper and consistent collection, processing, communication, use, and disposition of Personally Identifiable Information (PII) about cloud services.

22.2.8. Data stored with a cloud service provider or private hosting services should be encrypted during storage and transmission.

22.2.9. Cloud service providers and private hosting service providers shall be required to sign a Service Level Agreement with the State Department with enforceable penalties to ensure appropriate confidentiality, security, and availability of systems, data, and information is maintained.

22.2.10. Cloud service providers and private hosting service providers shall ensure that data, information, and systems are regularly backed up and copies provided to the State Department.

22.2.11. The State Department shall implement security capabilities for cloud services and private hosting services, including access control, confidentiality, integrity, and availability.

22.2.12. The System owner shall properly catalog their data and identify its sensitivity and the risk to the business of its leakage, loss, or corruption.

22.2.13. Contracts with cloud service providers shall include:

22.2.13.1. a clear definition of the Information Security responsibilities between them and the provider to ensure that all security aspects are covered, to avoid responsibility ambiguity.

22.2.13.2. An exit plan especially requiring the cloud provider to provide a way for the State Department to retrieve their systems, information, and data easily and economically;

22.2.13.3. Requirement for data sanitization from storage media, electronic and physical access rights be revoked from the cloud provider, and assets provided to the provider returned or, if not possible, be securely purged; and a Non-Disclosure Agreement signed;

22.2.13.4. Full disclosure in case of breaches to regulated information

22.2.13.5. Data ownership (the Government of Kenya to retain exclusive ownership of ALL data held in a cloud provider's solution entered by the State Department, systems, or affiliates in all media forms, e.g., online, backup and archive, etc.)

22.2.13.6. Data location (It should be explicitly stated in contracts that it should be in Kenya)

22.2.13.7. Service Level Agreements (to meet availability, performance, and disaster recovery requirements)

22.2.13.8. procedures for incident response and ensure that they meet the needs of the organization

22.2.13.9. Audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle

22.2.13.10. Provision for a Cloud Service Provider being taken over/bought-out by another organization (this should include providing the ownership and access rights, protection of any data the State Department owns and ensuring the data shall not be lost when there is a change of cloud service provider ownership)

23. Monitoring for Compliance

Information Security Policy compliance is both an operational and legal concern for organizations. The State Department must continuously monitor the implementation of the Information Security to ensure that it adheres to its ethical and legal responsibilities.

Maintaining Information Security compliance requires that an organization have well-defined programs, practices, and processes in place to review and reassess Information Security practices. To understand how the State Department's security program performs on a day-to-day basis, the Department must implement an Information Security Compliance Program to continuously monitor and document the implementation, effectiveness, adequacy, and status of all of their security controls.

Determination of applicable security policies, laws, and regulations is key. It will guide anyone carrying out compliance assessment in selecting the information to be collected and the type of compliance assessment methodology that should be performed.

23.1. Legal Requirements

23.1.1. Legal requirements include all Information Security activities relating to compliance with legal requirements.

23.1.2. All legislative obligations relating to Information Security shall be complied with and managed appropriately.

23.1.3. Each Directorate/Department/Section/Unit shall consider legislation and Policy-relevant to its business that could impact managing Information Security risks.

23.1.4. All Information Security policies, processes, and requirements, including contracts with third parties, shall be regularly reviewed for legislative compliance and the review results reported to the State Department.

23.1.5. Processes to ensure legislative compliance across all agency activities shall be developed and implemented.

23.2. Legal Context for Information Security in Kenya

23.2.1. **Constitution of Kenya (2010):** The Constitution of Kenya provides the supreme legal framework for information in Kenya. This is provided under Articles 11, 31(c & d), 33, 34, and 35. These provisions discreetly support information issues in the Country.

23.2.2. **County Government Act, 2012**: The Act (Part VIII and IX) provides for citizen participation, communication, and access to information at the county level and mechanisms for information and knowledge creation and sharing without discrimination of any kind.

23.2.3. **The InterGovernmental Relations Act, 2012**: The Act bestows the Council of Governors with a mandate to provide mechanisms for consultation amongst County Governments and for sharing information on counties' performance.

In the execution of stated functions. Section 5(d) provides for the establishment of a forum for sharing and disclosing necessary data and information.

23.2.4. **Kenya Information and Communication Act (Amendment Act) 2013**: This Act provides the main framework for regulating and facilitating the information and communications sector development. It is an amendment of the Kenya Information and Communications Act, 1998, the Principal Act.

23.2.5. **Access to Information Act, 2016**: The Act provides for routine and systematic information disclosure by public entities and private bodies on constitutional principles relating to accountability, transparency, and public participation and access to information.

23.2.6. **Data Protection Act, 2019**: Data Protection Act gives effect to Article 31(c) and (d) of the Constitution; and provides for the regulation of the processing, storage, and use of personal data.

23.2.7. **The Statistical Act, 2006 (Rev. 2019)**: The Act provides the collection, compilation, analysis, publication, and dissemination of statistical information.

23.2.8. **Kenya National Library Service Board Act, 1965 (Rev. 2012)**: This Act provides for promotion, establishment, equipping, management, maintenance, and development of libraries in Kenya as a National Library Service.

23.2.9. **Public Archives and Documentation Service Act, 1965 (Rev. 2012)**: The Act provides for the preservation of public archives and public records and a National repository for all knowledge work in Kenya by Kenyans and Kenya.

23.2.10. **The Evidence Act, 1963 (Rev. 2010)**: This Act gives officials wide discretion to decide whether (or not) the release of any information that they hold could be prejudicial to public Policy. This, in turn, affects the people, process, and technology approach of knowledge management.

23.2.11. **Copyright Act, 2001 (Rev. 2016)**: The Act makes provision for copyright in literary, musical, and artistic works, audio-visual works, sound recordings, broadcasts, and for connected purposes. This Act promotes the progress of science and useful arts by securing authors and inventors the exclusive right to their respective writings and discoveries for limited times.

23.2.12. **National ICT Policy of 2019**: It is a revision of the 2006 National ICT Policy and focuses on enhancing ICT infrastructure to conform with international standards, growing the contribution of ICT to the economy, positioning the Country to take advantage of emerging trends and gain global recognition for innovation, efficiency, and quality in public service delivery.

23.3. Policy Compliance

The Policy requirements domain includes all Information Security compliance activities relating to Information Security policies and the Government of Kenya's Information Security standards. All reporting obligations relating to SDP Information Security shall be complied with and managed appropriately.

23.4. Audit Requirements

23.4.1. The SDP audit requirements domain shall include all audit activities relating to Information Security activities.

23.4.2. All reasonable steps shall be taken to monitor, review and audit SDP Information Security compliance, including assigning appropriate security roles and engagement of internal and external auditors and specialist organizations where required.

23.5. Policy Review

23.5.1. The checklists provided for by the Government of Kenya Information Security standards shall be submitted as and when required for SDP current Information Security practices.

23.5.2. This Policy shall be reviewed as and when the need arises. Results of reviews shall be recorded, maintained, and reported.

23.6. Enforcement

23.6.1. Any employee found to have violated this Policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including termination of employment as per the PSC Code of Conduct and HR Policies Manual.

23.7. Information Security Policy Implementation

23.7.1. The implementation of the Policy shall be as per the implementation Matrix in Annex 1. The activities shall be incorporated in the work plans for the responsible Directorates, Departments, Sections and Units and budgeted for accordingly to facilitate implementation of the Policy.

23.7.2. The immediate activities to be undertaken to facilitate implementation of the Policy are:

1) Dissemination of the Information Security Policy;
2) Sensitization of Staff on the Information Security Policy;
3) Establish an Information Security Committee;
4) Appointment of Information Security Champions in Directorates, Departments, Sections and Units; and
5) Development of an Information Assets Register.

ANNEX

Annex 1: Information Security Policy Implementation Matrix

				TIMEFRAME (FY)																
				21/22		22/23				23/24				24/25				ESTIMATED COST (Kshs.)	INFORMATION SECURITY POLICY SECTION APPLIED	
S.No	ACTIVITIES	DELIVERABLE	RESPONSIBILITY	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4			REMARKS
1	Dissemination of the Information Security Policy	Dissemination Report	Administration and ICT		🟩													1,000,000	16. Personnel and Awareness.	Dissemination of Hard and Soft Copies of the Policy to Directorates/Departments /Sections/Units
2	Sensitization of Staff on the Information Security Policy	Sensitization Report	ICT Unit		🟩													2,000,000	16. Personnel and Awareness.	Sensitization of Staff should take place annually
3	Establish an Information Security Committee	Appointment Letters	Accounting Officer			🟩												_	2. Information Security Governance and Management.	
4	Appointment of Information Security Champions	Appointment Letters	Accounting Officer			🟩												_	2. Information Security Governance and Management.	
5	Carry out an Inventory of Information Assets	Information Asset Register	IS Committee, IS Champions, Internal Audit and ICT		🟩													2,000,000	3. Information Security Risk Management. 4. Resource Management. 6.2.3. Third-Party Service Delivery Policy	Information Asset Inventory Should be reviewed Annually
6	Develop and Information Security Risk Management (ISRM) Strategy	ISRM Strategy	IS Committee, IS Champions, Internal Audit and ICT			🟩												1,500,000	3. Information Security Risk Management.	

				TIMEFRAME (FY)																
				21/22		22/23				23/24				24/25						
S.No	ACTIVITIES	DELIVERABLE	RESPONSIBILITY	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	ESTIMATED COST (Kshs.)	INFORMATION SECURITY POLICY SECTION APPLIED	REMARKS
7	Conduct a Vulnerability Assessment and Risk Analysis ICT Systems and Information Assets	Vulnerability Assessment and Risk Analysis Report	IS Committee, IS Champions, Internal Audit and ICT				🟩											2,000,000	3. Information Security Risk Management. 4. Resource Management. 5. Physical and Environment Security. 6.2.3. Third-Party Service Delivery Policy 7. Network Security. 9. Electronic Information Transfer. 10.2.2. Computer Access Control. 14. Password Management.	
8	Develop a Risk Treatment Plan	Approved Risk Treatment Plan	IS Committee, Internal Audit and ICT				🟩											700,000	3. Information Security Risk Management. 4. Resource Management. 6.2.3.Third-Party Service Delivery Policy	
9	Document and Implement a Physical Security Plan	Physical Security Plan	Administration and ICT				🟩											_	5. Physical and Environment Security. 7.2.4.Boundary Protection Strategies.	
10	Equipment Maintenance, Tagging and Documentation	Equipment Maintenance Report, ICT Asset Inventory	Supply Chain Management & ICT Units				🟩	🟩										1,500,000	5. Physical and Environment Security. 7.2.5. Network Documentation. 7.2.8 Wireless Connections.	
11	Network Maintenance, Labelling and Documentation	Network Maintenance Report	ICT Unit						🟩	🟩								1,500,000	5. Physical and Environment Security, 7.2.5. Network Documentation. 7.2.8 Wireless Connections.	

S.No	ACTIVITIES	DELIVERABLE	RESPONSIBILITY	TIMEFRAME (FY)														ESTIMATED COST (Kshs.)	INFORMATION SECURITY POLICY SECTION APPLIED	REMARKS
				21/22		22/23				23/24				24/25						
				Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4			
12	Develop Access Management Procedures Manual	Access Management Procedures Manual	ICT and Record Management Unit					🟩										700,000	12. Bring Your Own Device. 13. Identity and Access Management. 14. Password Management. 15. Network Access.	
13	Review all system accounts, Password management for compliance and enforce Policy requirements	Identity and Access Management Report	ICT Unit						🟩									-	7. Network Security. 9. Electronic Information Transfer. 10.2.2. Computer Access Control. 14. Password Management.	This activity will be carried out quarterly
14	Document Incident and Event Management Procedures	Incident and Event Management Procedures Manual	Administration and ICT						🟩									1,200,000	17. Incident Management	
15	Maintain an Information Security Incident Register	Incident Register	Administration and ICT						🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	-	17. Incident Management	This activity will be continuous
16	Implement Network Monitoring Systems	Network Monitoring Systems	ICT Unit					🟩										2,000,000	7. Network Security	Monitoring System to be sourced.
17	Monitoring of the Network and Internet Usage	Network and Internet Monitoring Report	ICT Unit						🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	-	7. Network Security, 10.2.1. Internet Usage	Network Monitoring is continuous
18	Implement Anti-Virus Software	Anti-Virus Software installed and configured	ICT Unit	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	500,000	21. Malware Management	This activity is continuous
19	Develop a ICT Equipment Disposal Guide	ICT Equipment Disposal Guide	Supply Chain Management and ICT Unit					🟩										1,200,000	8. Information Technology Media Disposal Management	

				TIMEFRAME (FY)																
				21/22		22/23				23/24				24/25				ESTIMATED COST (Kshs.)	INFORMATION SECURITY POLICY SECTION APPLIED	
S.No	ACTIVITIES	DELIVERABLE	RESPONSIBILITY	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4			REMARKS
20	Document Change Management Procedures	Change Management Procedures Manual	Administration and ICT							🟩								700,000	18. Change Management	
21	Develop an Information and Systems Backup Programme and Procedures	Backup Programme, Back up Procedures	IS Committee				🟩											1,500,000	6.2.4 Backup Procedures 9.2.4. Recovering Emails. 12. BYOD. 22. Use of Cloud Services	
22	Implement Backup for Systems owned by the State Department	Backup Site in place	ICT Unit					🟩	🟩									2,500,000	5. Physical and Environment Security and 6.2.4 Backup Procedures	Equipment and software for the backup site to be acquired. Backup to be carried out at regular intervals
23	Development of a Business Continuity and ICT Disaster Recovery Plan	Business Continuity Plan	Internal Audit and IS Committee							🟩								1,500,000	19. Business Continuity 20. ICT Disaster Recovery	
24	Implementation and testing of the Business Continuity and ICT Disaster recovery Plan	Business Continuity Implementation Report	Internal Audit and IS Committee								🟩	🟩	🟩					5,000,000	19. Business Continuity 20. ICT Disaster Recovery	Acquisition of systems, facilities and equipment to facilitate business continuity
25	Implementation of Data Encryption Systems to appropriate Computing Systems	Encryption Systems Installation Report	ICT Unit									🟩	🟩					3,000,000	12. Bring Your Own Device 13. Identity and Access Management 14. Password Management 15. Network Access 22.Cloud Services	Data Encryption Software and relevant Keys to be acquired

S.No	ACTIVITIES	DELIVERABLE	RESPONSIBILITY	TIMEFRAME (FY)														ESTIMATED COST (Kshs.)	INFORMATION SECURITY POLICY SECTION APPLIED	REMARKS
				21/22		22/23				23/24				24/25						
				Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4			
26	Computer System Hardening	Computer Systems Hardening Plan and Report	ICT Unit					🟩										-	7. Network Security 12. Bring Your Own Device 13. Identity and Access Management 14. Password Management 15. Network Access	
27	Document ICT Operation procedures and responsibilities	ICT Operation Procedures Manual						🟩										1,000,000	6.2.1. Operational Procedures and Responsibilities 19. Business Continuity	
28	Implement a Configuration Management Database	Configuration Management Data Base	ICT Unit						🟩									1,500,000	7. Network Security. 18. Change Management.	
29	Review and Revise Information Security Policy	Revised Information Security Policy and Implementation Plan															🟩		23. 5 Policy Review	Proposed review of the Information Security Policy and Implementation Matrix after Three (3) years.