REPUBLIC OF KENYA

MINISTRY OF ROADS AND TRANSPORT

STATE DEPARTMENT FOR ROADS

DRAFT INFORMATION COMMUNICATION TECHNOLOGY POLICY

JANUARY 2026

Contents

ABBREVIATION AND ACRONYMS

ACL	Access Control List
AI	Artificial Intelligence
AP	Access Point
AU	African Union
AUP	Acceptable Use Policy
BCP	Business Continuity Plan
BETA	Bottom-Up Economic Transformation Agenda
BYOD	Bring Your Own Device
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
DHCP	Dynamic Host Configuration Protocol
DPIA	Data Protection Impact Assessment
DR	Disaster Recovery
EAC	East African Community
EBK	Engineers Board of Kenya
EDR	Endpoint Detection and Response
EDRMS	Electronic Document and Records Management System
GIS	Geographic Information Systems
GoK	Government of Kenya
ICT	Information and Communication Technology
IDP	Internal Digital Policy
IDS	Intrusion Detection System
IFMIS	Integrated Financial Management Information System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITS	Intelligent Transport Systems
KeNHA	Kenya National Highways Authority
KeRRA	Kenya Rural Roads Authority
KETRB	Kenya Engineering Technologist Registration Board
KICA	Kenya Information and Communications Act
KIHBT	Kenya Institute of Highways and Building Technology
KPI	Key Performance Indicator
KRB	Kenya Roads Board
KSh	Kenyan Shilling

KURA	Kenya Urban Roads Authority
LAN	Local Area Network
MAC	Media Access Control
MDA	Ministries, Departments and Agencies
MDM	Mobile Device Management
MERL	Monitoring, Evaluation, Reporting and Learning
MFA	Multi-Factor Authentication
MICDE	Ministry of Information, Communications and the Digital Economy
ML	Machine Learning
MoU	Memorandum of Understanding
MTP IV	Fourth Medium Term Plan
MTD	Mechanical and Transport Directorate
MTEF	Medium-Term Expenditure Framework
MTRD	Materials Testing and Research Directorate
NAC	Network Access Control.
NEMA	National Environment Management Authority
NGAV	Next-Generation Antivirus.
ODPC	Office of the Data Protection Commissioner
OECD	Organisation for Economic Co-operation and Development
PPP	Public-Private Partnership
PPADA	Public Procurement and Asset Disposal Act
PSC	Public Service Commission
R&D	Research and Development
RFP	Request for Proposal
SDGs	Sustainable Development Goals
SDLC	Software Development Life Cycle
SDoR	State Department for Roads
SLA	Service Level Agreement
SSID	Service Set Identifier
USB	Universal Serial Bus
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WiFi	Wireless Fidelity

CHAPTER 1

1.1 Vision

Be a global leader in the provision of cost-effective road transport infrastructure facilities.

1.2 Mission

To provide efficient, affordable, and reliable road transport infrastructure facilities for sustainable social and economic development.

1.3 Core Values

- Integrity: All staff shall uphold the highest standards of professional competence and integrity.
- Teamwork: The State Department is dedicated to teamwork and effective collaboration to achieve results
- Innovation: The State Department is committed to innovation and creativity in its leadership in the development of the infrastructure and the delivery of services.
- Customer focus: the State Department is committed to uphold customer driven and customer-focused service delivery.
- Inclusiveness and Equity: The State Department is committed to a consultative and participatory development process to ensure inclusiveness and equity in its service delivery.

1.4 Introduction

The State Department for Roads is the custodian of Kenya's most expansive physical asset, the national road network. As the country moves toward the realization of the Kenya National Digital Masterplan (2022–2032) and the Bottom-Up Economic Transformation Agenda (BETA), the State Department shall transition from a traditional infrastructure overseer to a digital-first governance entity. This Internal Digital Policy (IDP) serves as the official framework for institutionalizing technology within our workflows.

It is designed to ensure that the State Department does not merely "use computers," but operates as a data-driven organization capable of managing the "Digital Superhighway" alongside our physical roads. By digitizing our internal processes, we safeguard public funds, accelerate project delivery, and provide the transparency demanded by the Kenyan taxpayer.

1.5 Background

The State Department for Roads, established under Executive Order No. 1 of 2023 (as amended in 2025), is mandated to formulate policy and oversee the development, management, and maintenance of the national road network through its agencies, namely the Kenya National Highways Authority (KeNHA), Kenya Rural Roads Authority (KeRRA), and Kenya Urban Roads Authority (KURA), Kenya Roads Board (KRB), Engineers Board of Kenya (EBK) and Kenya Engineering Technologist a Registration Board (KETRB).

Functional and technical directorates under the State Department are as follows: Mechanical and Transport Directorate (MTD) to manage the mechanical and transport fund, Materials Testing and Research Directorate (MTRD) to conduct materials testing for roads infrastructure development, Kenya Institute of Highways and Building Technology (KIHBT) to build capacity for roads infrastructure development and the Roads directorate to coordinate agencies in the Road's sector.

The State Department receives significant support from its development partners mainly the World Bank which supports the Department and its beneficiary entities in the Road construction and capacity building which includes training of staffs support in ICT equipment's among others.

The State Department plays a critical role in enabling economic growth, regional integration, and access to social services by ensuring the availability of a safe, efficient, and reliable road network. Over the past decade, the national road network has expanded significantly to over 160,000 km, accompanied by increased complexity in planning, construction, maintenance, financing, and oversight. This expansion has resulted in the generation of large volumes of data, including road asset inventories, pavement condition assessments, traffic and axle load data, tolling and revenue information, environmental and social safeguards data, and contractor performance records. Traditionally, much of this information has been managed through manual processes and isolated digital systems, limiting its effective use.

The rapid advancement of digital technologies presents an opportunity to transform how the road sector operates. Technologies such as geographic information systems (GIS), remote sensing, mobile data collection, Intelligent Transport Systems (ITS), cloud computing, and data analytics can significantly improve asset management, project delivery, monitoring, and policy decision-making.

The absence of a unified digital policy has led to fragmented adoption of digital solutions, inconsistent data standards, duplication of systems, and challenges in interoperability and cybersecurity.

Furthermore, increasing expectations for transparency, accountability, and evidence-based decision-making require the State Department to treat data as a strategic asset. Without a clear policy framework on digital governance, data sharing, system integration, and investment prioritization, the State Department risks inefficiencies, higher operational costs, and underutilization of digital innovations.

The development of a digital policy for the State Department for Roads is therefore necessary to provide a coherent and coordinated framework to guide digital transformation across the State Department and its agencies. The policy shall establish principles for data governance, interoperability, cybersecurity, and digital service delivery; align digital initiatives with the strategic objectives; and ensure optimal use of ICT resources. Ultimately, the policy shall enable a data-driven, integrated, and resilient road sector capable of supporting sustainable development and improved service delivery.

1.6 Problem Statement

The rapid growth of Information and Communication Technologies (ICT) has led to increased generation, storage, and use of data across institutions and departments. However, the absence of a unified ICT policy has resulted in data fragmentation, where information systems operate in silos with limited interoperability. Critical data is dispersed across multiple platforms, formats, and ownership structures, making it difficult to access, integrate, analyze, and utilize data effectively for decision-making, service delivery, and strategic planning.

In addition, data-sharing concerns persist due to unclear data governance frameworks, lack of standardized protocols, and fears of related to data privacy, security, ownership, and misuse. Institutions often hesitate to share data because of legal ambiguities, weak data protection mechanisms, and the absence of trust and accountability structures. This limits collaboration, reduces operational efficiency, and undermines evidence-based planning and innovation.

Furthermore, ICT investments are implemented in an uncoordinated, duplicative, and not aligned with the State Department Strategic Plan 2023-2027. Significant resources are spent on standalone systems and infrastructure that do not integrate with existing platforms or scale easily to future needs.

This leads to inefficiencies, increased operational costs, underutilization of ICT assets, and limited return on investment. Furthermore, the absence or weak enforcement of ICT standards has resulted in heterogeneous systems that are not interoperable, secure, or scalable. Without common standards for hardware, software, data formats, cybersecurity, and system integration, the State Department face higher operational costs, increased security risks, and difficulties in integrating new technologies.

Without a comprehensive ICT policy to address these challenges, the State Department for Roads risks continued inefficiencies, data inconsistency, security vulnerabilities, and missed opportunities for digital transformation. There is therefore a critical need for a coherent ICT policy that promotes system interoperability, establishes clear data-sharing frameworks, strengthens data governance and security, and guides strategic, sustainable, and value-driven ICT investments.

1.7 Objective

To establish a coherent, secure, innovative, and sustainable digital governance framework that enhances service delivery, operational efficiency, regulatory compliance, and data-driven decision-making within the State Department for Roads.

1.7.1 Specific Objectives

i. To establish a structured ICT governance framework that ensures optimal planning, budgeting, prioritization, and utilization of digital resources across the State Department for Roads.
ii. To promote centralized coordination and interoperability of digital systems to reduce duplication, enhance integration, and ensure value for money in ICT investments.
iii. To align all digital initiatives with applicable laws and policies, including the Data Protection Act, 2019, the Computer Misuse and Cybercrimes Act (as amended), and relevant regional and international frameworks.
iv. To establish clear guidelines for data collection, storage, access, sharing, retention, and protection to safeguard sensitive information while enabling responsible data use within the State Department.
v. To create an enabling environment for the structured adoption of emerging technologies such as Artificial Intelligence, Internet of Things, machine learning, and big data analytics to improve road planning, construction, maintenance, and safety.
vi. To enhance awareness, skills, and competencies of staff in the use of digital tools and emerging technologies through continuous training, research, and capacity-building

programs.

vii. To provide clear guidelines for acquisition, utilization, maintenance, disposal, and environmentally sustainable management of ICT equipment in compliance with the Sustainable Waste Management Act.

viii. To define transparent and secure frameworks for collaboration with vendors, consultants, development partners, and other stakeholders to ensure accountability, data protection, and value creation.

ix. To transition innovation from isolated, individual-driven efforts to an institutionalized, policy-guided process that supports continuity, scalability, and sustainability.

x. To ensure availability, reliability, and continuity of digital services through robust business continuity and disaster recovery planning.

1.8 Rationale

This digital policy aims to enable the State Department to deliver efficient services, good governance and sustainable development by establishing a clear and coherent framework that shall guide adoption, governance and use of digital technologies.

Previously, the State Department has suffered from the lack of a strategic direction in the use of digital technologies, leading to the adoption of fragmented technology initiatives and, therefore, misalignment of digital investments with institutional and national goals.

This has led to inconsistencies in the application of digital technologies across the various divisions of the State Department. This policy seeks to address inefficiencies and ineffectiveness within processes by providing a framework for modernizing systems and automating manual and paper-based workflows in order to reduce costs, delays, and duplication while improving productivity and quality of services.

Cyber security has become a matter of national importance, and this policy is necessary to align practices in the state department with provisions of the Data Protection and other relevant acts of Parliament, to ensure compliance, in order to protect citizens, institutions and critical infrastructure while building public trust in digital systems

CHAPTER TWO: SITUATIONAL ANALYSIS

2.1 Overview

The State Department for Roads has made notable progress in the adoption of Information and Communication Technology (ICT) to support its mandate of planning, development, maintenance, and management of road infrastructure. A range of digital tools and systems are currently deployed to support administrative functions, financial management, procurement, communication, and selected technical operations. However, ICT adoption remains uneven, fragmented, and largely supportive rather than transformative.

Digitization initiatives to date have primarily focused on automating isolated processes as opposed to enabling integrated, end-to-end digital workflows. Consequently, this has constrained the Department's ability to operate in a data-driven, transparent, and responsive manner, particularly in areas such as project monitoring, road asset management, inter-departmental and inter-agency coordination, and evidence-based decision-making. Manual, paper-based, and semi-digital processes remain prevalent, especially in field operations and regional offices.

This chapter examines the current state of ICT and digitalization within the roads sub-sector, tracing its evolution, assessing prevailing practices, identifying key challenges, and highlighting gaps that necessitate the development of a dedicated ICT/Digital Policy. The analysis is anchored on Kenya Vision 2030, the Fourth Medium Term Plan (MTP IV), the Digital Economy Blueprint, and the National ICT Policy, 2019, and aligns with the Government's broader digital transformation agenda.

2.2 Evolution and Current Status of ICT and Digitalization in the Roads Sub-Sector

ICT has progressively become an integral enabler of public sector service delivery, including within the roads sector. In the early years, ICT adoption in road administration was largely limited to basic office automation, manual record-keeping supported by standalone computers, and the use of traditional communication channels.

With the introduction of cross-government digital platforms such as the Integrated Financial Management Information System (IFMIS), e-Procurement, and centrally managed human resource systems, the State Department for Roads transitioned into a more structured digital environment focused on accountability, compliance, and standardisation of public sector operations.

Subsequent investments in internet connectivity, email services, and basic networking infrastructure expanded access to digital tools at headquarters and selected regional offices. However, digitalization efforts remained largely compliance-driven and administrative in nature, with limited focus on digitizing core technical and operational road sector functions.

The launch of Kenya Vision 2030 and subsequent Medium-Term Plans underscored the importance of ICT as a catalyst for efficient infrastructure development and service delivery. While these frameworks encouraged sectoral digital transformation, the absence of a sector-specific digital policy for roads resulted in ad hoc system development, pilot initiatives, and fragmented solutions.

The rapid advancement of digital technologies, including geospatial systems, mobile data collection tools, sensors, and data analytics, has further exposed gaps in the Department's digital preparedness. As Kenya enters the final phase of Vision 2030 and implements MTP IV, the need for a coordinated and strategic digital approach in the roads sub-sector has become more pronounced.

2.3 Review of Policy, Legal and Institutional Frameworks

Kenya has established a robust overarching policy and legal framework to guide ICT and digitalization, including the Constitution of Kenya, 2010, the Kenya Information and Communications Act (KICA), the National ICT Policy 2019, the Digital Economy Blueprint, the Data Protection Act, 2019, Sustainable Waste Management Act 2022 and E-waste regulations 2024.

Institutionally, leadership on ICT matters is provided at the national level by the Ministry of Information, Communications and the Digital Economy, with Ministries, Departments and Agencies (MDAs) responsible for sector-specific implementation. The ICT Authority enforces ICT standards, develops and maintains shared ICT infrastructure systems, and provides oversight on electronic communications. Oversight institutions such as the Office of the Data Protection Commissioner (ODPC) ensure compliance with data protection and privacy requirements. Additionally, the National Environment Management Authority (NEMA) is responsible for regulating environmental aspects, including electronic waste (e-waste) management. These frameworks do not adequately address the specific operational, technical, and governance requirements of the roads sub-sector.

In particular, they provide limited guidance on system interoperability, sector-specific data governance, cybersecurity for infrastructure systems, and integration of digital technologies into core road functions.

2.4 Review of National, Regional and International Frameworks

At the national level, Kenya's development frameworks, including Kenya Vision 2030, the Fourth Medium Term Plan (MTP IV), the Bottom-Up Economic Transformation Agenda (BETA), and the National ICT Policy, emphasize digital transformation as a key enabler of efficient, transparent, and citizen-centered public service delivery.

Regionally, frameworks such as the African Union's Digital Transformation Strategy (2020–2030), the AU Data Policy Framework, the East African Community (EAC) Digital Transformation Strategy, and the broader EAC ICT Policy Framework promote the use of digital technologies to support infrastructure development, integration of digital markets, and economic growth. These frameworks emphasize harmonized policy and regulatory environments, cross-border data governance, cybersecurity, and system interoperability to enable seamless digital services, enhance regional integration, and expand digital trade across Member States.

Internationally, the United Nations Sustainable Development Goals (SDGs), particularly Goal 9 on resilient infrastructure and innovation and Goal 16 on effective, accountable institutions, underscore the importance of digital technologies in infrastructure development and governance. Frameworks and guidance from international organizations such as the World Bank's Digital Government and GovTech, OECD's Digital Government Policy Framework, and the International Telecommunication Union (ITU) demonstrate that sector-specific digital strategies in the roads sector significantly enhance asset management, project life cycle management, cybersecurity, transparency, and service quality.

These trends underscore the growing expectation for the roads sub-sector to adopt integrated and data-driven digital solutions aligned with national and global best practices.

2.5 Key Challenges, Gaps and Policy Implications

The situational analysis identifies several interrelated challenges and gaps constraining effective digital transformation within the State Department for Roads.

i. **Fragmented Digital Systems**: ICT systems operate in silos, resulting in duplication of effort, inconsistent data, and inefficiencies in service delivery.

ii. **Limited End-to-End Digitization**: Most processes are partially digitized, with critical workflows still dependent on manual interventions, especially in road construction, maintenance, and inspection activities.

iii. **Inadequate ICT Governance and Coordination**: Absence of a comprehensive digital governance framework has led to uncoordinated ICT investments, unclear roles, and weak oversight of digital initiatives.

iv. **Insufficient Skills and Change Management**: Limited digital skills, low awareness of emerging technologies, and inadequate change management have constrained effective adoption and utilization of ICT solutions.

v. **Weak Data Governance and Analytics Capability**: Lack of standardized data management practices limits the Department's ability to leverage data for planning, forecasting, monitoring, and evidence-based decision-making.

vi. **Infrastructure and Connectivity Gaps**: Unequal ICT infrastructure across headquarters, regional, and field offices affects consistency in service delivery and system usage.

vii. **Cybersecurity and Data Protection Risks**: Gaps in cybersecurity readiness expose the Department to risks related to data breaches, system downtime, and non-compliance with data protection requirements.

viii. **Unstructured Innovation and Partnerships**: Innovation initiatives are often driven by individuals rather than institutional priorities, and engagement with third parties lacks standardized guidelines.

The current ICT environment limits the Department's ability to operate efficiently, respond in real time, enhance transparency, and fully leverage data and digital technologies to improve road sector outcomes. Without a coordinated and strategic digital policy, the Department risks continued inefficiencies, increased operational costs, and missed opportunities for innovation and improved service delivery.

CHAPTER 3: POLICY STATEMENTS

The roads sub-sector is currently transitioning from traditional, paper-based operations to a modern digital ecosystem that prioritizes data sovereignty and real-time engagement. Historically, communication has been hindered by fragmented identity such as the use of personal emails for official business and passive websites that serve only as information boards. These gaps create significant cybersecurity risks and prevent a "single source of truth" for project tracking. Furthermore, the lack of integrated feedback loops means that critical citizen reports regarding road hazards, such as flooding or structural damage, often fail to reach the necessary technical teams in a timely or actionable manner.

To address these challenges, the internal ICT digital policy shall focus on standardizing institutional communication through mandatory official domains and verified social media presence to ensure authenticity and security. By implementing interactive citizen feedback platforms and centralized web dashboards, the sub-sector aims to move toward a "virtual office" model that shall reduce administrative red tape and documentation costs. This strategic shift shall transform communication from a simple support function into a proactive engineering tool, allowing for real-time hazard monitoring and greater public accountability across all road agencies.

3.1 ICT Governance

The State Department for Roads shall establish and maintain a robust ICT governance framework that aligns all digital initiatives with national priorities, ensures value for money, strengthens transparency and operational efficiency, mitigates risks, including cybersecurity and data integrity, promotes efficient resource utilization, and enforces performance measurement through clear KPIs, compliance audits, and reporting mechanisms to safeguard public trust. To operationalize this Policy Statement, the State Department for Roads shall:

i. **Governance Structures**

a) Establish a Directorate of ICT as guided by the Ministry of IC and Digital Economy.
b) Constitute a Digital Steering Committee chaired by the Principal Secretary to provide strategic oversight of ICT matters.
c) Create a Digitalisation Committee chaired by the Director ICT, comprising representatives from all departments, responsible for standards, interoperability, innovation pilots, monitoring compliance, and tracking digitalisation performance targets.

ii. **ICT Strategy and Planning**

a) Develop and periodically review a Digital Strategy/Policy aligned with national, regional, and global frameworks.
b) Require all ICT projects to undergo structured approval processes consistent with the Government of Kenya ICT governance standards.

iii. **Resource Allocation and Staffing**

a) Maintain adequate ICT staffing with defined competencies in infrastructure, applications, cybersecurity, data analytics, ITS, and emerging technologies.
b) Allocate sufficient funding for ICT operations, upgrades, maintenance, and innovation.

iv. **Procurement and Contracting**

a) Ensure all ICT procurement complies with the Public Procurement and Asset Disposal Act (PPADA, 2015).
b) Require Service Level Agreements (SLAs) with ICT service providers to guarantee availability, reliability, confidentiality, and integrity.

v. **Risk and Compliance Management**

a) Conduct annual ICT risk assessments and audits.
b) Ensure compliance with the Data Protection Act, Computer Misuse and Cybercrimes Act, and the Sustainable Waste Management Act.
c) Implement business continuity and disaster recovery plans for critical systems.

vi. **Performance Monitoring**

a) Establish KPIs for ICT projects and services, including uptime, user satisfaction, and cybersecurity incident reduction.
b) Publish quarterly ICT performance reports and conduct independent audits.

vii. **Capacity Building and Awareness**

a) Provide continuous training for all staff on ICT governance, application systems, cybersecurity, data governance, and emerging technologies.

b) Promote awareness campaigns to embed a culture of accountability, innovation and responsible digital practices.

3.2 Communications

The State Department for Roads shall ensure that all communications - network usage, email correspondence, social media, web presence, and citizen feedback platforms are secure, professional and compliant with national legislation and government standards.

3.2.1 Network and Internet Usage

The Department's internet infrastructure is a state-owned resource intended strictly for official duties.

i. Authorized Access: Access to the Department's network is restricted to registered devices only. Unauthorized tethering or use of third-party VPNs to bypass internal firewalls is prohibited.
ii. Monitoring: Under the 2025 Act, the Department reserves the right to monitor network traffic to detect "anomalous behavior" that may indicate a cyber-threat or a breach of the Critical Information Infrastructure (CII) protocols.

3.2.2 Official Email Correspondence

Email is the primary legal record for the Department's administrative decisions.

i. Exclusivity of @roads.go.ke: All official business shall be conducted via the assigned @roads.go.ke email address. The use of personal emails (Gmail, Yahoo, etc.) for official road project data or internal memos is a violation of this policy and the Data Protection Act (2019).
ii. Encryption and Digital Signatures: Emails involving sensitive procurement data, structural designs, or personnel files shall be encrypted.

In accordance with the Kenya Information and Communications (Amendment) Act, 2025, digital signatures shall be phased in as the only valid form of internal approval for financial commitments.

3.2.3 Verified Social Media and Web Presence

Social media is an essential tool for public updates on road conditions, closures, and project milestones.

i. **Account Verification:** The Department shall maintain only verified accounts (indicated by official badges) on platforms such as X (formerly Twitter), Facebook, and LinkedIn. No regional office or individual project team is permitted to create an "official" account without written authorization from the Director of Communications.
ii. **Combating Misinformation:** Under Section 30 of the 2025 Cybercrimes Act, spreading "false or misleading information" through official channels, even accidentally, carries heavy penalties. All posts shall be fact-checked against the Integrated Road Management System before publication.
iii. **Brand Uniformity:** All digital assets shall adhere to the National Government Brand Identity Manual, ensuring the public can easily distinguish authentic government communication from fraudulent "phishing" sites.

3.2.4 Citizen Feedback and E-Participation Platforms

To align with the BETA "Citizen-Centric" pillar, the Department shall institutionalize digital feedback loops.

i. **Interactive Portals:** The Department shall maintain a dedicated portal for reporting road defects (e.g., potholes, missing signage) and wayleave encroachments.
ii. **Data Privacy in Feedback:** While we encourage citizen engagement, all data collected through these platforms (Names, GPS locations, Phone numbers) shall be handled as "Sensitive Personal Data."
iii. **Response Timelines:** To ensure accountability, all feedback received through verified digital channels shall be acknowledged within 48 hours and resolved within the timelines specified in the Ministry Service Charter.

Policy Note on 2025 Compliance: Any employee found using official communication channels to engage in "Cyber Harassment" or the "unauthorized disclosure of CII data" shall be subject to both internal disciplinary action and criminal prosecution under the Computer Misuse and Cybercrimes (Amendment) Act, 2025, which now carries fines of up to Ksh 20 million.

3.3 Computer Hardware Policy

3.3.1 Policy Statement.

Information and Communication Technology (ICT) hardware forms a critical foundation for the delivery of government services, institutional efficiency, data security, and digital transformation within the public sector. In recent years, the State Department has experienced increased reliance on ICT hardware to support administrative operations, service delivery, data processing, inter-agency collaboration, and compliance with national digital governance initiatives.

Despite ongoing investments in ICT infrastructure, the absence of a standardized and comprehensive framework governing the acquisition, management, utilization, maintenance, and disposal of ICT hardware has resulted in operational inefficiencies and increased institutional risk. These gaps manifest in inconsistent procurement practices, inadequate asset tracking, unclear ownership and accountability, prolonged use of obsolete equipment, exposure to data breaches during disposal, and non-compliance with public procurement, environmental, and information security regulations.

Furthermore, rapid technological advancements and evolving cybersecurity threats require structured governance to ensure that hardware assets remain fit for purpose, cost-effective, secure, and aligned with approved institutional standards. The lack of defined lifecycle management processes also undermines value for money, sustainability objectives, and effective planning for replacement and upgrades.

This policy is therefore developed to address these gaps by establishing clear principles, roles, procedures, and controls for ICT hardware acquisition, management, and disposal. It seeks to promote transparency, accountability, security, standardization, and compliance with applicable laws, regulations, and government policies, while supporting the State Department's mandate for efficient, secure, and sustainable service delivery.

3.3.2 Policy guideline

3.3.2.1 Hardware Acquisition.

Acquisition of ICT equipment in the state department shall be guided by the Public Procurement and Disposal Act (2025).

The scope of equipment subject to procurement policies shall include end-user devices, networking devices, enterprise devices and peripherals sold or incorporated with the microprocessor.

3.3.2.2 Hardware Management.

Listed below are the hardware Management Guidelines as per the asset and liability management policy in the public sector, 2020.

A. Hardware Naming

These hardware naming guidelines apply to all servers, printers, workstations, and networking equipment owned or operated by the State Department. Unless otherwise stated, these guidelines are effective as of the issue date. The Hardware Naming guidelines shall take into consideration the following: (State Department/ funder/ Department/ Machine Category/ month/ year).

B. Hardware Inventory Control

These Hardware Inventory Control guidelines apply to all servers, printers, workstations, and networking equipment owned or operated by the State Department. Unless otherwise stated, these guidelines are effective as of the issue date.

All ICT equipment shall be recorded in the ICT asset register. This record shall include purchase date, Location of issued equipment, cost, assigned user, status and the warranty status. Periodic asset audits shall be conducted to verify records.

C. Hardware Installation and deployment.

These guidelines are on the identification of legitimate and prohibited hardware titles and outline proper measures for installation on computing devices. The purpose of this guideline is to reduce the risks of incompatible files or devices, malware, unlicensed software, and hacking that can result from unauthorized or infected software.

These guidelines may vary depending on the needs of the State Department, but it should openly communicate the roles and responsibilities of the users and the ICT staff.

i. The ICT Equipment shall be installed and configured by an authorised ICT personnel.

ii. The equipment shall be deployed in an environment that meets the manufacturer's recommended conditions.
iii. Critical equipment shall be protected by UPS and surge protection systems.
iv. Configuration and deployment details shall be documented.

D. Hardware Maintenance and Preventive Care.

The State Department shall ensure the provision of the ICT Services. Hardware maintenance support shall be provided in all areas under the State Department.

The ICT Department Shall:

i. Develop a preventive maintenance schedule.
ii. Perfom Regular cleaning, inspection, and performance checks in every quarter.
iii. Conduct firmware and hardware updates where necessary on a regular basis.
iv. Document all maintenance activities for reporting as per performance reporting guidelines.

E. Hardware Fault Reporting and Repair.

The State Department for Roads shall ensure:

i. The provision of timely reporting and repair of ICT equipment within the State Department as per the underlying guidelines.
ii. All hardware faults shall be reported immediately to the ICT Service Desk through official channels.
iii. Faults shall be logged in the ICT Asset and Incident Management System with a unique reference number for tracking.
iv. Authorized ICT personnel shall diagnose and repair faults in compliance with manufacturer specifications and departmental ICT standards.
v. Critical faults (servers, core networking devices) shall be escalated within 2 hours and resolved within 24 hours; non-critical faults shall be addressed within 48–72 hours.
vi. All repair activities shall be documented, including replaced parts, corrective actions, and technician details.
vii. Recurring faults shall be analyzed to inform preventive maintenance schedules and user sensitization.

viii. Unauthorized repairs or tampering with ICT equipment are prohibited and subject to disciplinary action.

3.4 Software Policy

3.4.1 Policy Statement.

Software systems are a critical enabler of government operations, service delivery, data management, and digital transformation within the public sector. State Departments increasingly rely on both in-house developed and externally acquired software solutions to support core administrative, operational, and service functions, as well as inter-governmental information exchange and automation of processes.

However, the expansion of software use has not been matched by a unified governance framework to guide the development, acquisition, licensing, deployment, maintenance, security, integration, and retirement of software assets. This has resulted in gaps, including fragmented development practices, duplication of systems, weak license and vendor management, unclear ownership of intellectual property, limited interoperability, inadequate documentation, and inconsistent application of cybersecurity and data protection controls, exposing the State Department to operational, legal, and security risks.

This policy provides a structured framework for the governance of both in-house developed and acquired software across their full lifecycle. It aims to ensure software solutions are secure, interoperable, sustainable, cost-effective, and legally compliant, while safeguarding institutional data, intellectual property, and service continuity, and supporting the State Department’s mandate for efficient, accountable, and digitally enabled service delivery.

3.4.2 Policy Guidelines

In line with the state department's objectives, below are listed policy guidelines.

A. Software Development (In-house)

i. Development shall follow approved **Software Development Life Cycle (SDLC)** methodologies.
ii. Rigorous testing in controlled environments is mandatory before deployment.

iii. Documentation (user manuals, technical specifications, maintenance guides) shall be maintained.
iv. Source code shall be securely stored in departmental repositories with controlled access.
v. Intellectual property rights of in-house developed software remain with the State Department for Roads.

B. Software Acquisition

i. Procurement shall comply with the **Public Procurement and Asset Disposal Act (2015).**
ii. Acquired software shall meet minimum technical requirements, security, and interoperability standards.
iii. Vendor contracts shall include **Service Level Agreements (SLAs)** covering support, updates, and compliance.
iv. All software licenses shall be provided, indicating the license period and the type.
v. Preference shall be given to scalable, cost-effective, and compatible solutions.

C. Hybrid Software Solutions

i. Hybrid systems shall integrate seamlessly with State Department's ICT infrastructure.
ii. Customizations shall be documented and approved by the ICT Committee.
iii. Maintenance responsibilities shall be clearly defined between in-house teams and vendors.
iv. Hybrid solutions shall comply with data protection and cybersecurity standards/ legal frameworks.

D. Software Security and Compliance

All software shall adhere to the Department's Cybersecurity Policy and national ICT security standards.

E. Software License Management and Control

i. All software licenses shall be centrally recorded and maintained within an approved ICT asset or license management register.

ii. License documentation, including agreements, certificates, renewal schedules, and proof of compliance, shall be securely retained for audit and accountability purposes.
iii. License usage shall be monitored to prevent over-deployment, misuse, or unauthorized installation.
iv. License reviews shall be conducted periodically to ensure optimal utilization and value for money.

F. Capacity Building.

i. Staff shall be trained on the use, security, and management of departmental software.
ii. Continuous professional development in software engineering and ICT innovation shall be encouraged.

G. Monitoring and Evaluation.

i. The State Department shall monitor software performance, usage, and compliance.
ii. Annual reviews shall assess relevance, efficiency, and alignment with departmental goals.
iii. Annual system audits shall be done to check compliance.
iv. Feedback mechanisms shall be established for users to report issues and suggest improvements.

3.5 Data Governance

The State Department of Roads is committed to complying with the Data Protection Act, 2019, and all applicable regulations issued by the Office of the Data Protection Commissioner (ODPC).

This policy establishes principles and controls governing the collection, use, access, retention, storage, and backup of data to ensure lawful, secure, and accountable handling of personal and operational data. While the policy demonstrates strong alignment with statutory requirements and best practices, gaps exist in operationalization, including but not limited to details on enforcement mechanisms, including staff capacity, standardized data classification, automation of retention and access controls, and measurable compliance indicators.

To address these gaps, the Department shall:

i. Strengthen implementation through clear standardized operating procedures.
ii. continuous staff training.
iii. Enhance role-based access and data classification schemes.
iv. regular Data Protection Impact Assessments
v. improved audit and monitoring tools.
vi. integration of data protection requirements into contracts and ICT systems
vii. Business continuity planning to ensure sustainable compliance and accountability
viii. Protection of personal and operational data.

The Department shall register as Data Controller and Data Processor, and ensure that all data processing activities are lawful, fair, transparent, and aligned with public interest and statutory mandates.

3.5.1 Data Collection

The Department shall ensure that:

i. Data is collected lawfully, fairly and transparently in accordance with Section 25 of the Data Protection Act, 2019.
ii. Only data that is relevant, adequate and limited to what is necessary.
iii. Personal data is collected for specified, explicit, and legitimate purposes, and data subjects should be informed of: -
    a) The purpose of data collection
    b) Their rights under the Data Protection Act
    c) How their data shall be used and protected
    d) Consent is obtained where required, except where data processing is permitted under public interest or legal obligation.

3.5.2 Data Use and Processing

The Department shall ensure that:

i. Data is used strictly for the purposes for which it was intended.

ii. Processing activities support service delivery, infrastructure development, policy formulation, compliance, and reporting.

iii. Data processing activities are documented, and **Data Protection Impact Assessments (DPIAs)** are conducted for high-risk processing activities.

3.5.3 Data Access and Sharing

The Department shall ensure that:

i. Access to data is granted on a need-to-know and role-based basis.

ii. Appropriate authentication and authorization controls implemented to prevent unauthorized access.

iii. Data sharing with other government agencies, contractors, or third parties shall be:

   a) Governed by formal agreements
   b) Limited to lawful and defined purposes
   c) Conducted in compliance with the Data Protection Act, 2019
   d) All data access and sharing activities are logged and audited.

3.5.4 Data Storage and Security

The Department shall ensure that:

i. Data is stored in secure systems, whether physical or logical, in line with Section 41 of the Data Protection Act.

ii. Appropriate technical and organizational measures implemented includes: -

   a) Encryption
   b) Secure servers and data centers
   c) Firewalls and intrusion detection systems
   d) Physical security controls

iii. Personal data is protected against loss, unauthorized access, alteration, disclosure, or destruction.

3.5.5 Data Retention and Disposal

The Department shall ensure that:

i. Data is retained only for as long as necessary to fulfill legal, regulatory, or operational requirements.

ii. Data retention schedules are defined and approved in line with:

a) Public Archives and Documentation Service Act, 2019

b) Data Protection Act, 2019

c) Government records management guidelines

iii. Upon expiry of the retention period, data is securely disposed of, Anonymized, and archived in accordance with approved archival procedures in accordance to Records Disposal Act, Cap 14, 2003.

3.5.6 Data Backup and Recovery

The Department shall ensure that:

i. Regular data backups are taken to support business continuity and disaster recovery.

a) Backups are securely stored, encrypted where applicable and Access-controlled

ii. Backup data is subject to the same data protection and retention requirements as primary data.

iii. Periodic testing of backup and recovery procedures is conducted to ensure data availability and integrity.

3.5.7 Data Subject Rights/access

The Department shall respect and facilitate data subject rights, not limited to: -

i. Right to access personal data

ii. Right to correction of inaccurate data

iii. Right to erasure where applicable

iv. Right to restriction or objection to processing

v. Right to lodge a complaint with the Office of the Data Protection Commissioner.

Procedures shall be in place to respond to data subject requests within statutory timelines.

3.6 ICT Security Policy

3.6.0 Problem Statement

The State Department for Roads has embraced Information and Communications Technology (ICT) as the key to the service delivery and management of the data, requiring high-level security to safeguard confidential information of the citizens despite the ever-changing and highly sophisticated threat environment. In the past, activities taken in addressing cybersecurity lacked cohesion, characterized by the lack of a guiding policy, uncertain governance, and the need for heightened resilience to be properly integrated in system lifecycles.

To fill these crucial gaps, the following ICT Security Policy introduces a cohesive, definitive policy to systematically migrate our entire enterprise from a strictly reactive, risk-managed, and resilience-oriented security environment to one that ensures consistent and proper protection of our various information assets.

3.6.1 Policy Governance

3.6.1.1 Purpose

This Cybersecurity Policy establishes mandatory requirements and procedures to protect the confidentiality, integrity, and availability (CIA Triad) of the STATE DEPARTMENT FOR ROADS information systems and data against internal and external threats in alignment with public trust and legal mandates.

3.6.1.2 Scope

This policy applies to:

i. All full-time, part-time, and temporary employees of the State Department.
ii. Contractors, consultants, vendors, and any third-party individuals with access to organizational IT resources.
iii. All information systems, networks, data (classified, sensitive, and public), hardware, and software owned, leased, or operated by the organization.
iv. All facilities housing IT assets or data.

3.6.1.3 Authority and Compliance

This policy is issued under the authority of the Principal Secretary. Its compliance is **mandatory**. Violations may result in disciplinary action, up to and including termination, and may carry civil or criminal penalties under relevant statutes (e.g., Data Protection Act 2019).

3.6.1.4 Policy Ownership

The State Department is the custodian of this policy. The ICT Department is responsible for policy maintenance, interpretation, and ensuring compliance.

3.6.1.5 Roles and Responsibilities

i. **Principal Secretary:** Ensures adequate resources and enforces accountability.
ii. **ICT Director:** Maintains policies/standards, oversees risk management, incident response, and continuous monitoring.
iii. **System Owners:** Ensure systems meet control requirements, maintain documentation, and validate access rights.
iv. **Employees and Users**: Comply with policy requirements and immediately report security incidents, protect credentials and devices.
v. **Contractors/Vendors**: Shall meet security requirements included in contractual agreements.
vi. **ICT Team**: Implements technical controls, conducts risk assessments, and manages incident response.

3.6.1.6 Monitoring

Use of ICT resources is subject to monitoring for compliance and security purposes.

3.6.1.7 Core Security Principles

All security activities shall be guided by these principles:

i. Security and continuity controls shall be integrated into the design and development of all systems and processes.
ii. Security decisions and investments shall be prioritized based on a continuous assessment of risk to mission, assets, and individuals.

iii. Multiple, layered security controls shall be employed to protect assets, ensuring no single point of failure.
iv. Users and systems shall be granted the minimum level of access necessary to perform their authorized functions.
v. Security is a collective duty shared by leadership, system owners, ICT professionals, and every user.
vi. The security program shall be regularly reviewed, tested, and updated based on lessons learned, threat intelligence, and performance metrics.

3.6.2 Acceptable Use Policy (AUP)

3.6.2.0 Problem Statement

The State Department for Roads ICT resources are essential for fulfilling its functions. They represent a significant investment and are a constant target for cyber threats. Unmanaged or inappropriate use creates security, legal, and reputational risks.

Prior to this policy, ambiguous guidelines led to inconsistent practices, including personal misuse of resources, introduction of unauthorized software, and exposure to non-work-related web threats, increasing malware infection risks and wasting public funds.

This policy establishes clear, enforceable boundaries for the use of all ICT assets. It defines acceptable and prohibited activities, ensuring resources are used responsibly, efficiently, and securely for their intended official purposes.

3.6.2.1 Policy Statement

ICT resources are provided for official government business. Incidental personal use is permitted only if it is minimal, does not interfere with duties, incurs no additional cost, or violates any law and complies with all aspects of this policy.

3.6.2.2 User Responsibilities

i. Use ICT resources only for purposes for which you are authorized.
ii. Prohibited activities include:
    a) Accessing, creating, storing, or transmitting offensive, harassing, or illegal material.
    b) Engaging in activities for personal financial gain (e.g., cryptocurrency mining, running a business).

c) Installing unlicensed software or circumventing security controls.
d) The input of sensitive or confidential data, including passwords into generative AI systems should be avoided as information entered may be stored, shared with other users and used to train the system.
e) Unauthorized access, interception, or monitoring of network traffic.
f) Posting organizational information on public forums/social media without authorization.

iii. Classify, handle, and transmit data according to its sensitivity level as defined in the Data Classification Policy.

3.6.3 Authentication Policy

3.6.3.0 Problem Statement

User credentials (usernames and passwords) are the primary gateway to our systems and data. Weak, reused, or compromised passwords are a leading cause of data breaches, allowing unauthorized access with significant impact. Previous password requirements were outdated, often leading to weak, easily guessed passwords or complex passwords that were difficult to remember and frequently used. A lack of Multi-Factor Authentication (MFA) for critical systems provided insufficient protection against credential theft. This policy modernizes our approach by implementing evidence-based, user-friendly standards aligned with international guidelines. It mandates strong passphrases, removes counterproductive frequent resets, and requires MFA for all remote and privileged access, dramatically increasing the difficulty for attackers.

3.6.3.1 Policy Statement

Strong authentication is required to protect systems and data. Passwords shall be complex, secret, regularly changed and securely managed.

3.6.3.2 Requirements

i. Password Creation:

a) Minimum of 8 characters for user accounts (12 characters is recommended), 15 for administrative accounts.
b) Use of a mixture of lower and uppercase characters, numeric, alphanumeric and special characters to promote complexity.

c) When creating passwords, do not use personal identifiable data, for example, name, date of Birth, Children's names, etc., as part of the password.
d) All user account passwords shall be changed frequently.

ii. Password Protection:

a) Passwords shall not be shared, written down, saved on the browser or stored in clear text.
b) Do not reuse passwords for organizational and personal accounts.
c) Use an appropriate password manager if needed.

iii. **Use of multi-factor authentication (MFA**) is mandatory where technically feasible for:

a) All remote network access (VPN).
b) All privileged administrative accounts.
c) Access to systems containing sensitive or classified information.

3.6.4 Bring Your Own Device (BYOD) Policy

3.6.4.0 Problem Statement

The proliferation of personal mobile devices has created user demand and operational efficiency opportunities to use them for work. However, uncontrolled personal devices accessing government data pose a severe and unmanaged risk to information security. There was no formal framework for securely integrating personal devices. This led to situations where employees accessed email and data on unsecured, unpatched devices with no oversight, risking data leakage and providing an unchecked entry point for malware. This policy establishes a controlled, risk-mitigated BYOD program. It mandates security pre-requisites, enrolment in a Mobile Device Management (MDM) system to enforce controls and separate work data, and clear rules of use, balancing flexibility with security.

3.6.4.1 Policy Statement

Limited, secure use of personally owned devices (smartphones, tablets, laptops) for official business may be permitted, provided they meet stringent security requirements to protect the organization’s data.

3.6.4.2 Eligibility and Requirements

i. Users shall obtain written approval from their supervisor and the ICT Department before using a BYOD for work.

ii. **Security Mandates for BYOD:**

   a) Device shall be password/PIN protected with auto-lock of not more than 5 minutes.

   b) Devices shall be configured with strong authentication and encryption.

   c) Operating system shall be kept current with vendor-supported versions and security patches.

   d) A reputable security app (anti-malware) shall be installed if applicable.

   e) Jailbroken/rooted devices are prohibited.

iii. Users shall report lost or stolen devices immediately. The State Department reserves the right to remotely wipe organizational data when necessary.

iv. All AUP rules apply when using a BYOD for work purposes.

3.6.5 Endpoint Protection Policy

3.6.5.0 Problem Statement

Malware (viruses, ransomware, spyware) is a pervasive and evolving threat designed to disrupt operations, steal data, or damage systems. Endpoints (laptops, workstations, servers) are the primary target for these attacks. Reliance on outdated or inconsistently deployed signature-based antivirus left gaps in protection. Lack of centralized management meant some systems were unprotected, definitions were not updated, and threat visibility was limited. This policy mandates the deployment of modern, centrally managed Endpoint Detection and Response (EDR) or next-generation antivirus across all assets.

Central management ensures real-time visibility, automated updates, and coordinated threat response, moving from passive detection to active prevention and hunting.

3.6.5.1 Policy Statement

All organizational ICT assets shall be protected by approved, centrally managed endpoint protection software to defend against malware, ransomware, and other threats.

3.6.5.2 Requirements

i. Organization-approved endpoint detection and response (EDR) or next-generation antivirus (NGAV) software shall be installed, enabled, and kept active on all servers, workstations, and mobile devices.
ii. Software shall report to a central security console managed by the ICT Department who shall monitor alert logs for infections and remediate as needed.
iii. Real-time (on access) scanning shall be enabled.
iv. Virus definitions and engine updates shall be configured to occur automatically at least daily.
v. Full system scans shall be performed weekly.
vi. Users shall not be able to circumvent, deactivate or install competing security software.
vii. Malware defence shall be complemented by application control/allow-listing on high-risk systems and by web filtering where appropriate.
viii. Malware incidents shall trigger containment, investigation, and eradication steps per the Incident Response Plan.

3.6.5.3 Exceptions

Any exceptions shall be justified, documented, and approved by the ICT Director.

3.6.6 Software Patching and Update Management Policy

3.6.6.0 Problem Statement

Vulnerabilities in software are the most common technical root cause of security incidents. The software supply chain itself is also a major attack vector. Unmanaged acquisition and slow patching create predictable, exploitable weaknesses. Software was often acquired without security considerations. No formal process existed to track assets or prioritize patching, leading to inconsistent update cycles, use of unsupported software, and exposure to known exploits for extended periods. This policy integrates secure acquisition with aggressive patch management. It mandates security requirements in procurement, maintains a software inventory, and establishes a risk-based timeline for remediating vulnerabilities, closing the window of opportunity for attackers.

3.6.6.1 Policy Statement

All software used by the State Department shall be acquired through a secure, authorized process and maintained with current security updates to minimize vulnerabilities.

3.6.6.2 Secure Software Acquisition Guidelines

i. All software purchases or downloads (including open source) require pre-approval from the IT department. Unauthorized software is prohibited.
ii. Security shall be a defined requirement in all procurement contracts and Request for Proposals (RFPs). Vendors shall commit to providing timely security patches for their products.
iii. For critical software, a basic assessment of the vendor's security practices is required before acquisition.
iv. All approved software shall be recorded in the State Department's central IT asset inventory.

3.6.6.3 Patching and Update Guidelines

All software and operating systems shall be kept current with security patches to mitigate vulnerabilities in a timely manner. A risk-based approach is used to prioritize updates. Timelines begin when a tested patch is released by the vendor.

i. **Critical/High-Risk Patches** (e.g for vulnerabilities being actively exploited): Apply within **14 days.**
ii. **Medium-Risk Patches:** Apply within 30 days.
iii. **Low-Risk and Standard Updates:** Apply within 60 days.
iv. **End-of-Life Software:** The use of unsupported software that no longer receives security patches is strictly forbidden. Exceptions require formal, documented approval from the Director ICT.
v. **Operating System and Major Software Updates:** Shall be planned and deployed within one vendor-supported version.

3.6.6.4 Patching and Update Process

Patching shall be managed centrally where possible. System owners are responsible for ensuring their systems are available for patching during maintenance windows.

i. IT shall test all patches in a separate environment before deployment.
ii. Updates shall be pushed centrally via management tools. System owners shall make systems available for maintenance.
iii. IT shall confirm successful patch installation.
iv. Any delay requires a documented risk acceptance form with a clear remediation date.

3.6.6.5 Secure Configuration and Hardening

i. Establish and maintain **secure baselines** for endpoints, servers, network equipment, and cloud resources; monitor for drift; remediate deviations.
ii. Implement least privilege, disable unnecessary services, enforce logging, and protect administrative interfaces (MFA + restricted access paths).

3.6.7 Email and Web Protection Policy

3.6.7.0 Problem Statement

Email, web services, and direct communication channels are essential but are commonly exploited by attackers using social engineering tactics. These attacks manipulate human psychology rather than technical flaws, making users the primary target for credential theft, malware attacks, and fraud. Phishing (email), vishing (voice), smishing (SMS), and other impersonation techniques pose a constant, high-risk threat. Previously, our defences were narrowly focused on email filtering, leaving gaps in awareness and response procedures for other manipulation tactics. This policy establishes a comprehensive defence against social engineering by combining robust technical controls across all channels with mandatory user training and clear reporting procedures.

3.6.7.1 Policy Statement

Email and web services are critical business tools that present significant attack surfaces. This policy shall establish mandatory security controls and user responsibilities to protect against email and web-based threats, particularly phishing, which is the primary vector for malware and data breaches.

3.6.7.2 Email Security

I. System-Level Protections

a) All inbound and outbound emails shall be filtered through the organization's approved cloud or on-premises security gateway.

b) All email attachments are scanned for malware. Suspicious file types (e.g., .exe, .scr, .js) shall be blocked or stripped.

c) All URLs in emails shall be scanned in real-time. Links to known malicious sites are blocked. Suspicious links may be rewritten to display a warning page before allowing access.

d) Technologies shall be configured to detect and quarantine emails that spoof the organization's domain or impersonate executives.

II. User Guidelines

a) Use only your official government email account for work-related communication. The format for the official email account shall be firstname.lastname@roads.go.ke

b) Be cautious of unexpected emails, especially those with urgent requests, unusual sender addresses, or grammatical errors.

c) Do not send sensitive or classified information via unencrypted email. Use designated secure file transfer systems.

d) Do not set up automatic forwarding of work email to personal accounts. Do not forward to all in situations that do not explicitly require you to do so

3.6.7.3 Web Security

i. Acceptable Use

a) Web access is provided primarily for official duties. Limited, incidental personal use is permitted if it complies with the Acceptable Use Policy.

b) Access to websites known for malicious content, hate speech, illegal activities, or excessive bandwidth consumption (e.g., video streaming for non-work) is prohibited.

ii. System-Level Protections

a) All web traffic shall be routed through a secure web gateway that filters content based on category and reputation, and blocks known malicious sites.

b) The gateway may inspect encrypted web traffic to detect threats hidden in encrypted sessions through SSL/TLS Inspection.
c) Organization-managed browsers shall be configured with the latest security settings, including disabling outdated plugins and extensions and enabling features like certificate pinning.

iii. **User Responsibilities**

a) Only interact with secure websites characterized by the use of https:// for any work-related activity. Verify the site's certificate if warnings appear.
b) Do not attempt to bypass web security filters using proxies, VPNs, or other methods.
c) Do not download files from untrusted websites. All downloads are subject to anti-malware scanning.

3.6.7.4 Social Engineering Protection

3.6.7.4.1 Scope of Social Engineering

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. This includes, but is not limited to:

i. **Phishing:** Fraudulent emails designed to trick recipients.
ii. **Vishing:** Fraudulent phone calls or voice messages impersonating trusted entities.
iii. **Smishing:** Fraudulent SMS/text messages containing malicious links or requests.
iv. **Pretexting:** Creating a fabricated scenario (e.g., impersonating IT support, a vendor, or a senior executive) to gain information or access.
v. **Baiting:** Offering something enticing (e.g., a free USB drive) to lure a victim into compromising security.
vi. **Quid Pro Quo:** Requesting sensitive information in exchange for a service or benefit.

3.6.7.4.2 Training and Awareness

i. All employees shall complete initial and annual security awareness training that covers all forms of social engineering.
ii. The ICT Department shall conduct periodic, controlled simulated social engineering exercises (e.g., phishing emails, test vishing calls) to reinforce training and identify areas for improvement.

3.6.7.4.3 Identification and Common Indicators

Users shall be vigilant for manipulation attempts across all communications. Common indicators include:

i. Messages creating a severe, immediate threat or an unexpected reward.
ii. Unsolicited requests for passwords, financial data, access codes, or other confidential data.
iii. Any communication claiming to be from a trusted source (IT, leadership, bank) but using unusual contact methods, tones, or email addresses.
iv. Requests to bypass normal policies, make unusual payments, or share credentials, even if they appear to come from a supervisor.
v. Slight misspellings in domains, unusual grammar, or caller IDs that seem similar to but not exact matches for legitimate numbers.

3.6.7.4.4 Reporting Procedure

i. Use the "Report Phish" button or forward the email as an attachment to the ICT Department.
ii. For Suspicious Calls/Visits: Politely end the interaction. Do not provide any information. Immediately report the incident to the ICT Department, providing details such as caller name, number, time, and the nature of the request.
iii. For Suspicious Text Messages: Do not click links or reply. Take a screenshot and report it to the ICT Department.
iv. General Rule: When in doubt, report it. Do not click, call back, or comply with the request until you have independently verified its legitimacy through a known, trusted method (e.g., call the official IT help desk number from the intranet).

3.6.7.4.5 Incident Response

i. Upon report, the ICT Department shall analyze the threat, block related malicious elements (URLs, numbers), and advise affected users.
ii. Users who inadvertently provided credentials, clicked a malicious link, or executed a file shall immediately change their password and contact the IT Service Desk for a security review.
iii. Attempted fraud or significant breaches shall be escalated per the Incident Response Plan.

3.6.8 Physical Security Policy

3.6.8.0 Problem Statement

Physical access to IT assets can bypass all network security controls. Servers, network equipment, and workstations are vulnerable to theft, tampering, or unauthorized access if not physically secured. Environmental hazards also pose a risk. Inconsistent physical security controls across facilities, lack of clean desk policies, and improper disposal of media containing sensitive data created risks of insider threat, loss, and environmental damage to critical infrastructure. This policy defines layered physical security controls for different areas (data centers, work areas), mandates secure disposal practices, and requires environmental protections for critical IT infrastructure to safeguard assets from physical threats.

3.6.8.1 Policy Statement

Physical access to IT assets shall be controlled to prevent unauthorized intrusion, theft, or environmental damage.

3.6.8.2 Requirements

i. Access to Data Centres and Server Rooms shall be restricted to authorized personnel via access control logs (keycard/biometric). Entry shall be logged, reviewed, and the visitors shall be accompanied.
ii. Employees shall practice "clean desk" policies for sensitive material. Workstations shall be locked when unattended. Laptops and mobile devices shall be physically secured with locking cables when in unsecured areas.
iii. All storage media (hard drives, USBs) shall be sanitized or physically destroyed prior to disposal or reuse.
iv. Critical IT facilities shall have monitored fire suppression, temperature, humidity controls and uninterruptible redundant power supply (UPS).

3.6.8.3 Surveillances System

Surveillance systems are deployed to enhance physical security, protect assets, deter criminal activity, and support incident investigations. This governs the proper use, monitoring, and management of surveillance systems to balance security needs with individual privacy rights.

i. **Deployment and Purpose**

a) CCTV cameras shall be installed in public areas, building exteriors, entry/exit points, data centers, server rooms, and other sensitive locations where there is no reasonable expectation of privacy.

b) Cameras are strictly prohibited in private areas such as restrooms, changing rooms, private offices (without explicit written authorization and notice), and any area where individuals have a reasonable expectation of privacy.

c) Primary Purposes:

i. Deterrence of theft, vandalism, and unauthorized access.

ii. Monitoring of secure areas and critical infrastructure.

iii. Investigation of security incidents and policy violations.

iv. Enhancement of employee and visitor safety.

ii. **Operation and Monitoring**

a) Surveillance systems shall be managed by the designated security personnel.

b) Monitoring is conducted for real-time incident response and shall be done where the general public or unauthorized staff cannot view it. Operators shall be trained in privacy compliance.

iii. **Signage and Notification**

a) Clearly visible signs shall be posted at all entrances to facilities and in areas where CCTV is deployed.

b) The signage shall include contact information for the office responsible for the CCTV system.

iv. **Data Management**

a) Recorded footage shall be retained for a minimum of **30 days**, unless retained as part of an active investigation, in which case it shall be preserved until the investigation concludes.

b) All footage shall be stored on secure, access-controlled systems with encryption at rest. Backups shall follow the State Department's data backup policy.

c) After the retention period, footage shall be securely erased in accordance with data retention guidelines for media sanitization.

d) Access to live feeds and recorded footage is strictly limited to:

i. Authorized security personnel for monitoring purposes.
ii. Law enforcement with a proper court order or warrant.
iii. Internal investigators with written approval from the Administration.

e) All access to and export of CCTV footage shall be logged and reviewed periodically.

v. **Incident Response and Evidence**

a) Footage related to a security incident shall be isolated and preserved immediately upon discovery.
b) Chain of custody procedures shall be followed for any footage used as evidence in disciplinary or legal proceedings.

3.6.9 Network Security Policy (Lan & Wireless)

3.6.9.0 Problem Statement

The State Department's local area network (LAN) and wireless infrastructure form the critical backbone for all internal and external communications and data flow. Unsecured network access provides a direct pathway for attackers to move laterally, eavesdrop on traffic, and compromise sensitive systems.

Historically, a flat network architecture with insufficient segmentation allowed unimpeded lateral movement. Wireless networks lacked strong encryption and guest isolation, creating an easy entry point. Network-level monitoring and access controls were inconsistently applied. This policy shall mandate a defence-in-depth architecture for all network layers. It requires network segmentation, strict access controls at the port and wireless level, continuous traffic monitoring, and the use of strong encryption to protect data in transit and contain potential breaches.

3.6.9.1 Policy Statement

All network infrastructure shall be configured and maintained to provide a secure, segmented, and monitored environment. This applies to both wired (LAN) and wireless network access, ensuring the confidentiality and integrity of network traffic and restricting access to authorized users and devices only.

3.6.9.2 Core Requirements

i. **Network Architecture & Segmentation:**

a) A defined network segmentation strategy (e.g., separate zones for servers, users, guests, and Internet of Things devices) shall be implemented using firewalls or Virtual LANs with access control lists (ACLs).

b) A "deny-all" rule shall be the default stance between network segments, with access permitted only by business-justified exception.

ii. **Wired LAN Security:**

a) Switch ports shall be configured with port security features (e.g., Media Access Control (MAC) address limiting, Dynamic Host Configuration Protocol (DHCP) snooping) where feasible.

b) Unused network ports in public or insecure areas shall be administratively disabled.

c) Network Access Control (NAC) should be implemented to authenticate devices before granting network access.

iii. **Wireless Security:**

a) All organization-controlled WiFi networks shall use the latest strong encryption standard (e.g. WIFI Protected Access (WPA3)). Open (unencrypted) Wi-Fi for general staff use shall be prohibited.

b) A separate, logically isolated guest wireless network shall be provided for visitors and personal devices. Guest network traffic shall have no access to the internal organizational network.

c) Broadcast of SSIDs should be configured appropriately (e.g., hidden for sensitive networks). SSID names shall not reveal sensitive organizational information.

d) All wireless access points shall be secured with changed default credentials, placed in monitored locations, and have remote management disabled.

iv. **Network Monitoring & Defense:**

a) All network traffic shall be logged, with logs retained for a minimum of 90 days to support investigations.

b) Intrusion Detection/Prevention Systems (IDS/IPS) shall be deployed at key network boundaries to monitor for and block malicious activity.

c) Regular vulnerability scans of network infrastructure (switches, routers, firewalls) shall be performed.

v. **User Responsibilities**

a) Users shall not install unauthorized wireless routers, access points, or network hardware and shall result to confistication.

b) When using organizational Wi-Fi, users shall only connect to the official, IT-provisioned SSIDs.

c) Users shall treat wired network ports as secure assets and not connect unauthorized devices.

3.6.10 Security Incident Reporting and Response

3.6.10.0 Problem Statement

Security incidents are inevitable. The speed and effectiveness of the response directly determine the extent of damage, data loss, and operational disruption. A disorganized response exacerbates the impact and complicates legal and public reporting obligations. No formal, well-communicated incident response plan existed. Employees were unsure how or when to report suspicious activity, leading to delayed detection and response.

Roles and procedures for containment and investigation were undefined. This policy shall establish a clear, simple reporting pathway for all personnel and define the structured response process for the security team. It ensures swift action to contain damage, eradicate threats, recover operations, and meet all regulatory notification requirements.

3.6.10.1 Policy Statement

All suspected or confirmed security incidents shall be reported immediately to facilitate a rapid, coordinated response to minimize impact.

3.6.10.2 Definition of an Incident

Any real or suspected event that compromises the confidentiality, integrity, or availability of an information system or the data, for example, malware infection, data breach, lost device, unauthorized access, or denial of service.

3.6.10.3 Reporting Procedure

i. **Immediate Action:** Upon discovery, the individual shall:

a) Immediately contact the ICT Office.

b) If possible, isolate the affected system from the network (unplug Ethernet/turn off Wi-Fi) without powering it down.

c) DO NOT investigate or alter the system beyond containment.

ii. **ICT Security Office:** Shall activate the Incident Response Plan, containing the threat, eradicating it, recovering systems, and conducting a post-incident review.

iii. **Communication:** The DICT and Communication office shall manage internal and external notifications as required by law and regulation.

3.7 Emerging Technologies

The State Department for Roads shall adopt and integrate emerging technologies, including Artificial Intelligence (AI), Internet of Things (IoT), Machine Learning (ML), Big Data Analytics, among others, as strategic tools to enhance efficiency, transparency and innovation in its operations. Adoption shall be guided by ethical principles, compliance with national legislation, and benchmarking against global best practices.

3.7.1 Policy Guidelines

i. **Responsible Adoption**

a) All emerging technology deployments shall comply with the Data Protection Act (2019), Computer Misuse and Cybercrimes Act (2018/2025), and relevant international ethical standards.

b) AI and ML systems shall be designed with transparency, fairness, explainability and human oversight to prevent bias and misuse.

ii. Capacity Building

a) Continuous training shall be provided to staff on AI, IoT, ML, and data analytics, reducing reliance on individual champions and embedding institutional knowledge.

b) Partnerships with development partners, donors, universities, research institutions and private sector innovators shall be pursued to accelerate adoption and build expertise through hackathons, use case simulations among others.

3.8 ICT User Management Policy

3.8.1 Policy Statement.

The State Department relies extensively on ICT systems, applications, and digital platforms to support governance, service delivery, data management, and collaboration among internal and external stakeholders.

As these systems increasingly handle sensitive government information and personal data, effective management of user access rights is essential to protect information assets, maintain system integrity, and ensure continuity of operations. Proper user rights management underpins accountability, auditability, and trust in public sector digital services.

The absence of a standardized and consistently enforced user management framework has exposed gaps in access control practices. These gaps include inconsistent user provisioning and de-provisioning processes, excessive or inappropriate access privileges, delayed revocation of access following role changes or separation, limited periodic access reviews, and inadequate segregation of duties. Such weaknesses increase the risk of unauthorized access, data breaches, misuse of ICT resources, non-compliance with data protection requirements, and challenges in attributing responsibility for system actions.

This policy is therefore established to address these gaps by providing a structured framework for the granting, management, review, and revocation of user access rights across all ICT environments. The policy seeks to ensure that access to systems and information is strictly role-based, formally authorized, regularly reviewed, and promptly withdrawn when no longer required, thereby strengthening information security, enhancing accountability, and supporting efficient, compliant, and secure public service delivery.

3.8.2 Definitions

Term	Definition
User	Any individual authorized to access ICT systems
Access Rights	Permissions assigned to perform system actions
Privileged Account	Account with administrative or elevated rights

Least Privilege	Granting minimum access required for duty
Third Party	External entity granted temporary access

3.8.3 User Categories and Role Assignment

i. Users shall be classified based on functional roles.
ii. Access rights shall be assigned strictly in line with approved job responsibilities.
iii. Segregation of duties shall be enforced to prevent conflict of interest.

3.8.4 Account Creation and Authorization

i. All user accounts shall be created following written approval.
ii. Authorization shall involve the immediate supervisor, Human Resource function, and the ICT Department.
iii. Shared or generic accounts are prohibited except where formally justified and approved.

3.8.5 Access Rights and Privilege Management

i. Access shall be granted on a need-to-know and need-to-use basis.
ii. Privileged access shall be strictly limited and logged.
iii. Users shall not escalate privileges without authorization.

3.8.6 Authentication and Credential Management

i. Users shall be issued with unique credentials.
ii. Password and authentication controls shall comply with the Authentication Policy.
iii. Credential sharing is prohibited. Users shall be held liable for any faults.

3.8.8 User Access Rights Review and Monitoring

i. User access rights shall be reviewed periodically.
ii. System activity logs shall be maintained for audit and investigation.
iii. Unauthorized access attempts shall be reported immediately.

3.8.9 Account Modification and Role Changes

i. Access rights shall be updated promptly following changes in role or duty station as informed by the HR Department.
ii. Temporary privilege elevation shall be time-bound and approved.

3.8.10 Account Suspension and Revocation

i. Access shall be revoked immediately upon separation from service.

ii. Dormant accounts shall be disabled.

iii. Emergency suspension may be enforced where security risks exist.

3.8.11 Third-Party and Temporary Access

i. Third-party access shall be contract-based, time-bound, and supervised.

ii. Access shall be revoked upon contract expiry or task completion.

3.8.12 Data Protection and Confidentiality

i. Access to personal and sensitive data shall comply with the Data Protection Act, 2019.

ii. Confidentiality obligations shall survive separation from service.

3.8.13 Incident Management and Violations

i. Access-related incidents shall be reported and investigated.

ii. Corrective and disciplinary actions shall be applied where violations occur.

3.8.14 Enforcement Matrix

Area	Responsible Office	Enforcement Action	Review Frequency
User account approval	Supervisor / HR / ICT	Access validation	On request
Privileged access	ICT |Department	Logging and audit	Quarterly
Dormant accounts	ICT Department	Disable / delete	Monthly
Policy violations	HR / Internal Audit	Disciplinary action	As required
Third-party access	ICT / Procurement	Contract enforcement	Per contract

3.8.15 User Account Recovery

User-friendly account recovery features shall be employed. Developed and procured systems shall have “Do-it-yourself” password recovery features.

3.8.16 User Access Approval Workflow

i. User Request Initiated

↓

ii. Supervisor Approval

↓

iii. HR Verification (status/role)

↓

iv. ICT Department Account Provisioning

↓

v. User Acknowledgement of ICT Policies

↓

vi. Periodic Review / Audit

3.8.16 ISO/IEC 27001 and GOVERNMENT DIGITAL SUPERVISION MAPPING (Annex)

Policy Clause	**ISO/IEC 27001 Control**	**Government Alignment**
User access control	A.5.15	GoK ICT Security Standards
Least privilege	A.5.18	Public Service ICT Governance
Authentication	A.5.17	National Cybersecurity Framework
Logging and monitoring	A.5.28	Government Digital Supervision
Access revocation	A.5.19	PSC Exit Management Guidelines
Data confidentiality	A.5.34	Data Protection Act, 2019
Third-party access	A.5.22	Government Procurement Rules
Incident management	A.5.25	National CERT Guidelines

3.9 Business Continuity Plan (BCP) Policy

The State Department for Roads is committed to ensuring the continuous delivery of its critical functions and services. This Business Continuity Plan (BCP) Policy affirms the Department's commitment to preparedness, resilience, and effective response to disruptions that may arise from natural disasters, technological hazards, pandemics, security threats, or other emergencies.

Currently, the Department lacks a fully documented, approved, and standardized business continuity management framework, where backup measures are ad-hoc and not uniformly applied across the departments.

The Department recognizes that disruptions to operations, information systems, or key infrastructure can significantly affect service delivery, public safety, and economic disruption. As such, this policy shall establish, implement, and maintain a structured Business Continuity Management plan that ensures the timely recovery and continuity of essential services and functions.

In this regard, the following provisions shall apply:

i. The State Department shall undertake periodic risk assessments to determine the criticality, dependencies, and recovery priorities of ICT systems and data.
ii. Data backup criteria, including backup frequency, retention periods, and recovery objectives, shall be defined and documented to guide the data restoration process.
iii. Physical and analogue records of operational value shall be progressively converted into digital format to support secure backup, preservation, and archival.
iv. Backup media shall be stored in secure locations that are fireproof, waterproof, and have adequately protected against unauthorized access.
v. A standardized naming and classification convention for backup files and folders shall be adopted to enhance traceability, retrieval, and management of backup data.
vi. A hybrid storage architecture comprising on-premise and offsite storage facilities shall be established and maintained to support resilience and effective data recovery.
vii. All application data shall be backed up using daily incremental backups and weekly full backups, or as determined by system criticality.
viii. System-level data, including configurations, audit logs, and security logs, shall be backed up at least once every month.

ix. Electronic records shall be retained and disposed off in accordance with the applicable Records Management Policy and legal requirements.

x. A hot site or equivalent high-availability recovery environment for critical systems and applications shall be established and maintained to ensure rapid service restoration.

xi. Data recovery and system restoration tests shall be conducted periodically to assess the effectiveness, reliability, and readiness of backup and recovery arrangements.

xii. All data back-up and recovery facilities shall be located in secure environments with appropriate physical, logical, and environmental controls, in alignment with ISO 22301 and ISO/IEC 27001 standards.

xiii. The State Department shall document all incidents, disruptions, and system or data restoration procedures to support accountability, audit, and continuous improvement.

xiv. Data centres supporting critical systems shall implement fully redundant architectures, including power, network, storage, and cooling systems, as a precautionary measure to enhance availability and resilience.

Through this policy, the State Department for Roads commits to building a resilient organization capable of withstanding disruptions and sustaining critical operations in order to fulfil its mandate and serve the public effectively.

3.10 Training, Research and Capacity Building

To achieve its mandate, the State Department for Roads recognizes the need for digital training, capacity building, and development for all staff. These initiatives are pillars of sustainable development and effective service delivery; they continuously strengthen staff knowledge, skills, and competencies, ensuring the State Department remains responsive, innovative, and impactful.

This policy shall emphasize on training, research, and capacity building, outlining the HR and ICT Department commitment to develop the skills, knowledge, and institutional strength required to effectively adopt and manage digital technologies in the State Department for Roads.

The State Department currently faces critical challenges in training, research, and capacity building. These include: inadequate funding for infrastructure; limited capacity in emerging technologies; insufficient succession planning and knowledge transfer; inadequate monitoring and

evaluation of training impact; and a shortage of specialized technical skills. These deficiencies result in underperformance and inefficiencies in service delivery.

To achieve the objectives, the State Department shall:

i. Build digital competencies among staff.

ii. Promote high-quality digital research and innovation.

iii. Strengthening institutional capacity through digital tools and systems.

iv. Encourage responsible, ethical, and secure use of digital technologies.

v. Support continuous learning and adaptation to emerging technologies.

vi. Collaborate with development partners, international organizations and regional bodies for core funding.

3.11 Document management

Effective document management is critical for accountability, institutional memory, service delivery, and compliance within Government. State Department for Roads is committed to maintaining a secure, efficient, and compliant digital document management system.

Currently, document management practices lack clear guidelines for the creation, storage, access, retention and disposal of all digital documents, standardized classification scheme, consistent file indexing and loss of documents. Additionally, the State Department also lacks a disaster recovery plan. These hinder efficient information retrieval, data protection, knowledge sharing and timely decision making, necessitating the need to establish a coherent, secure, and standardized document management policy.

To achieve the above objectives, the state department shall:

i. Develop clear guidelines for the creation, storage, access, retention and disposal of all digital documents.
ii. Develop and implement a standardized file classification scheme and file plan.
iii. Implement an Electronic Document and Records Management System (EDRMS).

iv. Strengthen data security by using access controls, audit trails and backup mechanisms.

3.12 Partnerships and Collaborations

The State Department for Roads shall foster strategic partnerships and collaborations with public, private, academic, and international stakeholders to accelerate digital transformation in the roads sector. Partnerships shall be guided by transparency, accountability, and alignment with national priorities to ensure that innovation, resources, and expertise are mobilised effectively and sustainably.

3.12.1 Policy Guidelines

i. **Public–Private Partnerships (PPPs)**

a) Establish PPP frameworks for the deployment of Intelligent Transport Systems (ITS), smart tolling, and digital twins, which are currently domiciled in Semi-Autonomous Government Agencies (SAGAs), but there is a need for State Department leadership)

b) Ensure PPP contracts include clear performance targets, data governance provisions, and compliance with national ICT standards.

ii. **Academic and Research Collaborations**

a) Partner with universities and research institutions to advance Research and Development (R&D) in AI, IoT, machine learning, and big data analytics for road infrastructure.

b) Support innovation labs and pilot projects to test emerging technologies before full-scale deployment.

iii. **International and Regional Cooperation**

a) Engage with international organisations and regional bodies to harmonise standards, share best practices, and enable cross-border interoperability of digital road systems.

b) Benchmark against global leaders in digital infrastructure to continuously improve Kenya's digital roads ecosystem.

iv. **County Government Engagement**

a) Collaborate with county governments to integrate local road inventories, citizen feedback platforms, and GIS systems into national digital frameworks.
b) Provide technical support and capacity building to ensure county-level systems meet national standards.

v. **Private Sector Innovation**

a) Encourage partnerships with technology firms to co-develop solutions for predictive maintenance, traffic optimisation and e-waste management.
b) Require all collaborations to comply with the Data Protection Act, cybersecurity regulations, and sustainable waste management laws.

vi. **Transparency and Accountability**

a) All partnerships shall be formalised through Memoranda of Understanding (MoUs), contracts, or framework agreements with clear roles, responsibilities, and reporting obligations.
b) Performance of partnerships shall be monitored through Key Performance Indicators (KPIs) and published in annual reports to ensure accountability and public trust.

CHAPTER FOUR: POLICY IMPLEMENTATION FRAMEWORK

4.1 Introduction

This chapter provides the framework for implementing the ICT Policy of the State Department for Roads. It outlines the coordination structures, administrative mechanisms, legal and regulatory alignment, funding arrangements, and supporting measures necessary to ensure effective, sustainable, and accountable digital transformation. The framework is designed to operationalize the policy objectives, guarantee compliance with national and international standards, and deliver measurable outcomes in service delivery, efficiency, and transparency.

4.2 Coordination Framework

Effective implementation of the ICT Policy requires harmonized coordination across the State Department and stakeholders in the roads sub-sector.

i. **Digital Steering Committee**: Chaired by the Principal Secretary, responsible for strategic oversight, prioritization of ICT investments, and alignment with national digital transformation agendas.
ii. **ICT Department**: Established within the State Department to provide technical leadership, policy oversight, and operational guidance on ICT matters.
iii. **Digitalisation Committee**: Chaired by the Director ICT, comprising representatives from all directorates and agencies. This committee shall oversee standards, interoperability, innovation pilots, compliance monitoring, and performance tracking.
iv. **Stakeholder Engagement**: Development partners, vendors, and citizen representatives shall be engaged through structured consultative forums to ensure inclusiveness, transparency, and accountability.

4.3 Administrative Mechanisms

Administrative structures shall ensure efficient execution, accountability and sustainability of ICT initiatives.

i. **Strategic Planning**: All ICT projects shall be integrated into the State Department's Strategic Plan and annual work plans.
ii. **Approval Processes**: ICT initiatives shall undergo structured appraisal and approval consistent with Government ICT governance standards.
iii. **Performance Management**: Key Performance Indicators (KPIs) shall be established for ICT projects, covering system uptime, user satisfaction, cybersecurity incident reduction, service delivery timelines and other relevant parameters.
iv. **Capacity Building**: Continuous training programs shall be rolled out to enhance staff competencies in emerging technologies, cybersecurity, and data governance.
v. **Change Management**: Structured change management programs shall be implemented to build awareness, reduce resistance, and embed a culture of innovation and accountability.
vi. **Business Continuity**: Disaster recovery and continuity plans shall be developed for all critical ICT systems to ensure resilience.

4.4 Legal and Regulatory Framework

Implementation of the ICT Policy shall be anchored on compliance with national, regional and international legal instruments.

i. **National Laws**:
    a) Constitution of Kenya, 2010 (Articles 10 and 232 on values, transparency, and accountability).
    b) Kenya Information and Communications Act (KICA).
    c) Data Protection Act, 2019.
    d) Computer Misuse and Cybercrimes Act (as amended, 2025).
    e) Public Procurement and Asset Disposal Act, 2015.
    f) Sustainable Waste Management Act, 2022 and E-Waste Regulations, 2024.

ii. **Regional Frameworks**:
    a) African Union Digital Transformation Strategy (2020–2030).
    b) East African Community ICT Policy Framework.

iii. **International Frameworks**:

a) Relevant ISO Standards

All ICT initiatives should comply with these frameworks to ensure legality, interoperability, and alignment with global best practices.

4.5 Funding Arrangements

Adequate and sustainable financing is critical for successful implementation.

i. **Government Budgetary Allocations**: ICT projects shall be integrated into the Medium-Term Expenditure Framework (MTEF) and annual budgets.

ii. **Development Partner Support**: Continued collaboration with partners such as the World Bank for capacity building, ICT equipment, and technical assistance.

iii. **Public-Private Partnerships (PPPs)**: Structured engagement with private sector actors to co-finance innovation, infrastructure, and service delivery platforms.

iv. **Cost Optimization**: Adoption of shared services, cloud computing and centralized procurement to reduce duplication and achieve economies of scale.

v. **Sustainability Measures**: ICT investments shall incorporate lifecycle costing, environmentally sustainable procurement, and e-waste management compliance.

CHAPTER 5: MONITORING, EVALUATION, REPORTING AND LEARNING (MERL)

i. **Monitoring**: Quarterly ICT performance reports shall be published, covering KPIs, compliance audits, and user feedback.

ii. **Evaluation**: Evaluations shall be conducted biannually to assess effectiveness, efficiency and impact.

iii. **Reporting**: Annual ICT implementation reports shall be submitted to the Principal Secretary

iv. **Learning**: Lessons learned shall be documented and disseminated to inform future ICT initiatives and policy reviews.

v. **Risk Management**:

a) **Cybersecurity Risks**: Regular risk assessments and penetration testing to safeguard critical information infrastructure.

b) **Operational Risks**: Business continuity planning to mitigate system downtime.

c) **Financial Risks**: Transparent procurement and audit mechanisms to prevent misuse of funds.

d) **Environmental Risks**: Compliance with e-waste regulations to mitigate environmental harm.

CHAPTER 6: POLICY REVIEW AND UPDATE

The ICT Policy shall be reviewed every three years to incorporate emerging technologies, evolving legal frameworks, and lessons learned from implementation.

ANNEX

Annex 1: Definition of Terms

Term	Definition
Artificial Intelligence (AI)	The use of computer systems capable of performing tasks that normally require human intelligence, including learning, reasoning, prediction, and decision-support.
Business Continuity Plan (BCP)	A documented framework that guides the continuity and recovery of critical operations and ICT systems in the event of disruption.
Cloud Computing	The delivery of computing services, including servers, storage, databases, networking, and software, over the internet on demand.
Cybersecurity	The practice of protecting ICT systems, networks, and data from unauthorized access, cyber threats, attacks, or damage.
Data	Raw facts, figures, symbols, or records collected and processed by the State Department for Roads in the course of its operations.
Data Governance	The framework of policies, standards, roles, and processes that ensure effective, secure, and lawful management of data throughout its lifecycle.
Data Protection	Measures and processes applied to safeguard personal data in accordance with the Data Protection Act, 2019.
Data Subject	An identifiable natural person to whom personal data relates, as defined under the Data Protection Act, 2019.
Digital Transformation	The integration of digital technologies into institutional processes to improve efficiency, transparency, service delivery, and decision-making.
Digitalization	The strategic use of digital technologies to fundamentally transform business models, processes, and customer experiences
Digitization	Converting analog to digital
Electronic Waste (E-waste)	Discarded electrical or electronic equipment and components, managed in accordance with environmental and waste management laws.
ICT	Technologies used for the creation, storage, processing, transmission, and dissemination of information, including computers, networks, and software.
ICT Governance	Structures, processes, and decision-making mechanisms that ensure ICT investments align with institutional objectives and national priorities.

Information System	An organized set of ICT components used to collect, process, store, and disseminate information.
Intelligent Transport Systems (ITS)	Integrated digital technologies applied to transport infrastructure and vehicles to improve safety, efficiency, and traffic management.
Interoperability	The ability of different ICT systems and platforms to exchange data and operate seamlessly with one another.
Internet of Things (IoT)	A network of physical devices embedded with sensors and connectivity that enable data collection and exchange.
Personal Data	Information relating to an identified or identifiable individual, as defined under the Data Protection Act, 2019.
Policy	A set of principles, rules, and guidelines adopted by the State Department to guide decision-making and operations.
Stakeholder	Any individual, organization, or entity with an interest or role in the implementation of the ICT/Digital Policy.
System Interoperability	The capability of ICT systems to communicate, share data, and function across institutional and sectoral boundaries.

Annex2: Policy Implementation matrix

Policy Objective	Strategies / Activities	Responsible Actors	Timeframe	Performance Indicators	Resources Required
Establish a structured ICT governance framework	- Constitute Digital Steering Committee - Form Digitalization Committee	Principal Secretary, Director ICT,	2026–2027	- Committees established and meeting quarterly	Budget for committee operations
Promote centralized coordination and interoperability of digital systems	- Adopt interoperability standards - Integrate agency systems into central platform - Conduct compliance audits	Directorate of ICT, ICT Authority	2026–2028	- % of systems integrated - Annual compliance reports - Reduction in duplicated ICT projects	ICT infrastructure, technical consultants, audit tools

Policy Objective	Strategies / Activities	Responsible Actors	Timeframe	Performance Indicators	Resources Required
Align digital initiatives with applicable laws and policies	- Review ICT projects for legal compliance - Train staff on Data Protection Act & Cybercrimes Act - Establish compliance reporting mechanism	Directorate of ICT, ODPC, Legal Directorate	Continuous (2026–2030)	- % of projects legally compliant - Number of staff trained - Annual compliance reports submitted	Training budget, legal advisory services
Establish clear guidelines for data governance and security	- Develop data governance framework - Implement standardized data collection/storage protocols - Conduct annual cybersecurity audits	Directorate of ICT, ODPC, MICDE	2026–2027	- Approved data governance framework - % of systems with standardized protocols - Annual audit reports	Cybersecurity tools, training, consultancy
Adopt emerging technologies (AI, IoT, Big Data, ITS)	- Identify AI use cases for the SD - Pilot AI-enabled systems, Innovations - Train staff on emerging technologies	Directorate of ICT, MTD, MTRD, KIHBT	2027–2030	- Number of use cases identified -Number of pilots implemented - % of staff trained - ITS systems operational	ICT equipment, training funds
Enhance staff awareness and competencies	- Continuous ICT training programs - Capacity-building	Directorate of ICT, KIHBT, HR Directorate	Annual (2026–2030)	- Number of staff trained - Training satisfaction	Training budget, partnerships,

Policy Objective	Strategies / Activities	Responsible Actors	Timeframe	Performance Indicators	Resources Required
	workshops - Partnerships with training institutes			scores - Partnerships established	e-learning platforms
Ensure sustainable ICT equipment lifecycle management	- Develop ICT Asset Inventory - Implement asset tracking system - Enforce e-waste disposal compliance	Directorate of ICT, Procurement Unit, Asset Disposal Committee	2026–2028	- ICT Asset register - % of assets tracked - Compliance with e-waste regulations	ICT asset management system, disposal contracts
Strengthen collaboration with stakeholders	- Establish vendor management framework - Sign MoUs with development partners - Hold annual stakeholder forums	Directorate of ICT, Administration, legal, Procurement Unit, Development Partners	2026–2030	- Vendor framework operational - Number of MoUs signed - Annual forums held	Stakeholder engagement funds, meeting facilities
Ensure availability and continuity of digital services	- Develop disaster recovery plans - Implement business continuity systems - Conduct resilience testing	Directorate of ICT, ICT Authority, Finance, Procurement	2026–2029	- Approved DR plans - % of critical systems with continuity measures - Annual resilience test reports	Backup systems, cloud services, technical staff

Annex 3: Monitoring & Evaluation Matrix

Policy Objective	Key Indicators	Means of Verification	Frequency of Measurement	Responsible Actors	Assumptions / Risks
Establish ICT governance framework	- Steering & Digitalisation Committees functional	- Committee minutes - Annual reports	Quarterly	Principal Secretary, Director ICT	Risk of delays in approvals; assumption of political support
Promote interoperability of digital systems	- % of ICT systems integrated - Reduction in duplicated ICT projects	- Integration audit reports - compliance assessments	Bi-annual	Directorate of ICT, ICT Authority/MICDE	Risk of resistance from USERS; assumption of adequate funding
Ensure legal compliance of ICT initiatives	- % of projects compliant with Data Protection Act - Number of staff trained	- Compliance audit reports - Training attendance records	Annual	Directorate of ICT, ODPC, Legal Directorate	Risk of weak enforcement; assumption of continuous legal updates
Strengthen data governance and security	- Approved data governance framework - % of systems with standardized protocols - Number of cybersecurity incidents reduced	- Policy documents - Cybersecurity audit reports - Incident logs	Annual	Directorate of ICT, ODPC, ICT Authority	Risk of cyber-attacks; assumption of adequate technical capacity

Policy Objective	Key Indicators	Means of Verification	Frequency of Measurement	Responsible Actors	Assumptions / Risks
Adopt emerging technologies (AI, IoT, ITS)	- Number of pilots implemented - % of staff trained	- Pilot project reports - Training records	Annual	Directorate of ICT, MTD, MTRD, KIHBT	Risk of rapid tech obsolescence; assumption of partner support
Enhance staff competencies	- Number of staff trained - Training satisfaction scores - Partnerships established	- Training records - Feedback surveys - MoUs signed	Annual	Directorate of ICT, KIHBT, HR Directorate	Risk of staff turnover; assumption of continuous training budget
Ensure sustainable ICT equipment lifecycle management	- Hardware policy approved - % of assets tracked - Compliance with e-waste regulations	- Policy documents - Asset registers - NEMA compliance reports	Annual	Directorate of ICT, Procurement Unit, Asset Disposal committee, NEMA	Risk of poor disposal practices; assumption of enforcement of e-waste laws
Strengthen stakeholder collaboration	- Vendor framework operational - Number of MoUs signed - Annual forums held	- Vendor contracts - MoUs - Forum reports	Annual	Directorate of ICT, Legal, Procurement Unit, Development Partners	Risk of weak partnerships; assumption of stakeholder buy-in
Ensure continuity of digital services	- Disaster recovery plans approved - % of critical systems with	- DR plans - Continuity test reports - ICT Authority assessments	Annual	Directorate of ICT, ICT Authority, Agency ICT Departments	Risk of system downtime; assumption of adequate ICT infrastructure

Policy Objective	Key Indicators	Means of Verification	Frequency of Measurement	Responsible Actors	Assumptions / Risks
	continuity measures - Annual resilience test reports				

Annex 4: ICT Risk Management Matrix

This Annex provides a structured ICT Risk Management Matrix for the State Department for Roads. It identifies, assesses, and prescribes mitigation measures for risks associated with the use, management, and governance of Information and Communication Technology (ICT) in support of the Department's mandate.

This Annex applies to all ICT systems, infrastructure, services, data, users, and third-party service providers within the State Department for Roads, including headquarters, regional offices, and project sites.

ICT risks shall be assessed using the following criteria:

4.1 Likelihood

i. **Low (L):** Unlikely to occur
ii. **Medium (M):** Possible occurrence
iii. **High (H):** Likely or frequent occurrence

4.2 Impact

i. **Low (L):** Minimal disruption to operations
ii. **Medium (M):** Noticeable disruption requiring management intervention
iii. **High (H):** Severe disruption to service delivery, compliance, or reputation

4.3 Risk Level

Risk level shall be determined by combining likelihood and impact and categorized as:

i. **Low**
ii. **Medium**
iii. **High**
iv. **Critical**

4.4 ICT Risk Management Matrix

4.4.1 Strategic and Governance Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures	Responsible Office
ICT-01	Misalignment of ICT initiatives with departmental mandate and national transport strategy	M	H	High	Alignment of ICT strategy with national and sector policies; periodic policy reviews	Director, ICT
ICT-02	Inadequate ICT governance and accountability structures	M	H	High	Establishment of an ICT Steering Committee; defined roles and responsibilities	Principal Secretary
ICT-03	Insufficient ICT budget allocation	H	H	High	Integration of ICT planning into MTEF and annual budgets	Finance & ICT

4.4.2 Operational Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures	Responsible Office
ICT-04	System downtime affecting road project management and reporting	M	H	High	Redundant systems; service level agreements; disaster recovery planning	ICT Operations
ICT-05	Failure of ICT systems	M	H	High	Preventive maintenance;	ICT & User Departments

	supporting road asset management				system audits; data backup procedures	
ICT-06	Inadequate ICT skills among staff	H	M	High	Continuous ICT training and capacity building	Human Resource & ICT

4.4.3 Cybersecurity and Information Security Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures	Responsible Office
ICT-07	Cyberattacks on ICT systems	H	H	Critical	Implementation of cybersecurity controls; monitoring and incident response	ICT Security
ICT-08	Data breaches involving sensitive government information	M	H	High	Data classification; encryption; access controls	ICT Security
ICT-09	Unauthorized access to ICT systems	M	H	High	Role-based access control; strong authentication mechanisms	ICT Security

4.4.4 Legal and Regulatory Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures	Responsible Office
ICT-10	Non-compliance with the Data Protection Act, 2019	M	H	High	Data protection policy; appointment of a Data Protection Officer	Legal & ICT
ICT-11	Non-compliance with ICT Authority standards and guidelines	M	M	Medium	Adoption and enforcement of GoK ICT standards	ICT

ICT-12	Breach of software licensing agreements	M	M	Medium	Software asset management and audits	ICT & Procurement

4.4.5 Financial Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures	Responsible Office
ICT-13	Cost overruns in ICT projects	M	H	High	Use of approved project management frameworks	ICT & Procurement
ICT-14	Procurement fraud in ICT acquisitions	M	H	High	Compliance with procurement laws; internal and external audits	Procurement & Internal Audit

4.4.6 Technology and Infrastructure Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures	Responsible Office
ICT-15	Obsolescence of ICT infrastructure	H	M	High	ICT lifecycle management and upgrade planning	ICT
ICT-16	Inadequate network connectivity in remote project sites	H	M	High	Use of hybrid connectivity solutions	ICT
ICT-17	Failure of backup and disaster recovery systems	M	H	High	Off-site backups; periodic disaster recovery testing	ICT

4.4.7 Reputational and Service Delivery Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures	Responsible Office
ICT-18	Public dissatisfaction due to ICT service disruptions	M	H	High	ICT service desk; incident management procedures	ICT

ICT-19	Loss of public trust due to misuse of information	M	H	High	Enforcement of data governance and accountability	Management & ICT

Annex 5: Environmental Risk Management Matrix

To identify, assess, and manage environmental risks associated with the generation, handling, storage, transportation, and disposal of electronic waste (e-waste), in compliance with applicable environmental laws and regulations, and to mitigate adverse environmental and public health impacts.

5.1 Applicable Legal and Regulatory Framework

- Environmental Management and Coordination Act (EMCA), Cap 387
- Environmental Management and Coordination (Waste Management) Regulations
- Sustainable Waste Management Act, 2022
- National E-Waste Management Guidelines
- Occupational Safety and Health Act, 2007
- Any other applicable Government of Kenya policies and standards

5.2 Environmental Risk Management Matrix (E-Waste Compliance)

5.2.1 Regulatory and Compliance Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation / Control Measures	Responsible Office
ENV-01	Non-compliance with national e-waste regulations	M	H	High	Adoption of an e-waste management policy; compliance audits	ICT & Environment Officer
ENV-02	Failure to obtain approvals or	L	H	Medium	Engagement of licensed e-waste handlers	Procurement & ICT

	licenses for e-waste disposal				approved by NEMA	
ENV-03	Poor documentation of e-waste disposal activities	M	M	Medium	Maintenance of disposal records and certificates of destruction	ICT

5.2.2 Environmental Impact Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation / Control Measures	Responsible Office
ENV-04	Environmental pollution due to improper disposal of ICT equipment	M	H	High	Segregation of e-waste; disposal through licensed recyclers	ICT & Environment Officer
ENV-05	Soil and water contamination from hazardous components	L	H	Medium	Secure storage; safe handling procedures	ICT
ENV-06	Air pollution from unsafe dismantling or burning of e-waste	L	H	Medium	Prohibition of informal disposal practices	Management

5.2.3 Occupational Health and Safety Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation / Control Measures	Responsible Office
ENV-07	Exposure of staff to hazardous substances in e-waste	M	H	High	Use of PPE; staff training on safe handling	ICT & OSH Committee
ENV-08	Injuries during handling or storage of obsolete ICT equipment	M	M	Medium	Safe storage facilities; handling guidelines	ICT

5.2.4 Operational and Reputational Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation / Control Measures	Responsible Office
ENV-09	Accumulation of obsolete ICT equipment due to delayed disposal	H	M	High	Periodic e-waste disposal schedules	ICT
ENV-10	Reputational damage due to poor environmental stewardship	M	H	High	Public compliance with environmental standards; reporting	Management

5.2.5 Supply Chain and Third-Party Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation / Control Measures	Responsible Office
ENV-11	Engagement of unlicensed e-waste recyclers	M	H	High	Due diligence and verification of service providers	Procurement
ENV-12	Non-compliance by contracted service providers	M	H	High	Contract clauses on environmental compliance; monitoring	Procurement & ICT

Annex 6: Captive Portal Policy

6.1 Introduction

A captive portal is a network access control mechanism that intercepts users' attempts to access the internet or internal resources and redirects them to a designated web page for authentication, authorization, or acceptance of terms and conditions. Captive portals are implemented to ensure secure and controlled access to the organization's network, protect sensitive information, and manage network usage in compliance with applicable policies and regulations.

This policy defines the purpose, scope, and responsibilities associated with the use of captive portals, establishing guidelines for authorized access, monitoring, and enforcement.

All users accessing the organization's network through a captive portal are required to comply with this policy to maintain the integrity, confidentiality, and availability of network resources.

6.2 Purpose

The purpose of this policy is to:

i. Ensure that all users accessing the organization's network through a captive portal are authorized.
ii. Protect the organization's network and data from unauthorized access or misuse.
iii. Establish clear user responsibilities for compliant and secure use of network resources.
iv. Provide a framework for monitoring and enforcing captive portal access and usage.

6.3 Scope

This policy applies to:

i. All employees, contractors, guests, and third-party users accessing the organization's network via the captive portal.
ii. All network devices, including wired, wireless, and remote connections subject to captive portal control.
iii. All data transmitted or received over the network when using captive portal access.

6.4 User Responsibilities

Users accessing the network through a captive portal shall:

i. Complete all required authentication steps before accessing network resources.
ii. Review and accept all terms and conditions presented on the captive portal.
iii. Use the network in accordance with organizational policies, applicable laws, and regulations.
iv. Protect their login credentials and not share them with unauthorized individuals.
v. Immediately report any suspicious activity, security incidents, or potential unauthorized access to the IT security team.
vi. Refrain from attempting to bypass or circumvent the captive portal controls.

6.5 Acceptable Use

While connected to the network via a captive portal, users shall ensure their activities are:

i. **Authorized:** Accessing only permitted resources for legitimate business purposes or approved activities.
ii. **Secure:** Avoiding the transmission of sensitive information over unsecured connections unless encryption (e.g., HTTPS, VPN) is used.
iii. **Compliant:** Not engaging in illegal, harmful, or disruptive activities, including but not limited to:
    a) Unauthorized access to other users' accounts or data
    b) Distribution of malware or malicious software
    c) Excessive use of bandwidth that negatively impacts other users
    d) Activities that violate intellectual property rights or privacy regulations

6.6 Enforcement

i. The State Department reserves the right to monitor and log network access and usage through the captive portal for security, compliance, and auditing purposes.
ii. Non-compliance with this policy may result in:
    a) Temporary or permanent suspension of network access
    b) Disciplinary action in accordance with organizational policies

c) Legal action if laws or regulations are violated

iii. IT and security teams are responsible for enforcing this policy, responding to incidents, and ensuring compliance with internal and external standards.

The State Department for Roads is committed to ensuring secure and reliable access to its ICT systems. This policy establishes standardized procedures for user account recovery, enabling authorized users to regain access efficiently while safeguarding sensitive information and preventing unauthorized use.