REPUBLIC OF KENYA

MINISTRY OF INFORMATION, COMMUNICATIONS AND THE DIGITAL ECONOMY

STATE DEPARTMENT FOR ICT AND THE DIGITAL ECONOMY

KENYA CLOUD POLICY (2025) IMPLEMENTATION GUIDELINES

JUNE 2026

Table of Contents

ACRONYMS iv
EXECUTIVE SUMMARY vii
FOREWORD ix
ACKNOWLEDGEMENT x
CHAPTER ONE: INTRODUCTION 1
1.1 Background 1
1.2 Purpose 1
1.3 Scope 2
1.4 Rationale 2
CHAPTER TWO: OVERVIEW OF CLOUD COMPUTING 3
2.2 Policies and Legal Framework 3
2.4 Current State 3
2.5 Challenges: 9
i. Limited resources 9
ii. Security Risks 9
iii. Data Silos 10
iv. Disaster Recovery 10
v. Compliance and regulatory requirements 11
2.6 International Best Practices 11
i. International Governance Framework 11
ii. Codes of Conduct for Responsible Use of cloud computing services: 12
iii. Data Interoperability and Portability 12
iv. Global standardization 12
CHAPTER THREE: POLICY STATEMENT 18
3.2 Statements 18
CHAPTER FOUR: IMPLEMENTATION AND GOVERNANCE 21
4.1 Implementation Strategy 21
4.1.1 Migration Strategy 21
4.1.2 Considerations for Cloud Policy 23
i. Cybersecurity 23
ii. Technical 25
iii. Commercial 26
4.1.3 Contract Terms 28

4.1.4 Skills and Capabilities 31
4.1.5 Vendor Lock-in 35
4.1.6 Vendor Management 36
4.1.7 Data Classification 38
4.1.8 Registration of Cloud Service Providers 40
CHAPTER FIVE: MONITORING, EVALUATION AND REVIEW 47
5.1. Monitoring, and evaluation 47
5.1.1 Risk management 48
5.1.2 Risk mitigation 49
5.2 Effective date of review 50
APPENDICES 51
APPENDIX I: THE CLOUD MIGRATION ROADMAP AND PHASE MIGRATION TIMELINE 51
APPENDIX II: CONTRACT DRAFTING CHECKLIST – ENTITY ↔ GCSP AGREEMENTS 66
APPENDIX III. ACCREDITATION FRAMEWORK FOR GCSP TECHNICAL AND SECURITY STANDARDS APPLICABLE FOR CLOUD BASED ON DATA CATEGORIZATION 76
APPENDIX IV: FRAMEWORK FOR ACCREDITATION OF CLOUD SERVICE PROVIDERS GCSP AND NON-GCSP APPROVAL 79
APPENDIX V: CLOUD COMPLIANCE SELF -EVALUATION MATRIX. 82
APPENDIX VI: LOCATION TRANSPARENCY TEMPLATE 85

ACRONYMS

ACLs	Access Control Lists
AI	Artificial Intelligence
Anti-DDoS	Anti–Distributed Denial of Service
API	Application Programming Interface
AWS	Amazon Web Services
BCP	Business Continuity Plan
BETA	Bottom-up Economic Transformation Agenda
BI	Business Intelligence
Bi-Monthly	Occurring every two months
BYOL	Bring Your Own License
CAC	Cloud Adoption Committee
CapEx / CAPEX	Capital Expenditure
CD	Compact Disc
CDMI	Cloud Data Management Interface
CEO	Chief Executive Officer
CI	Continuous Integration
CMCA	Computer Misuse and Cybercrimes Act
COTS	Commercial Off-The-Shelf
CRM	Customer Relationship Management
CS	Cabinet Secretary for ICT
CSP	Cloud Service Provider
CSV	Comma-Separated Values
CTO	Chief Technology Officer
DC	Data Centre
DDoS	Distributed Denial of Service
DE	Digital Economy
DPA	Data Protection Act
DR	Disaster Recovery
DRP	Disaster Recovery Plan
ERP	Enterprise Resource Planning
GCSP	Government Cloud Service Provider
GoK	Government of Kenya
Gov-Cloud	Government Cloud
HR	Human Resource
HRIS	Human Resource Information System
IaaS	Infrastructure as a Service
IAM	Identity and Access Management

ICT	Information and Communication Technology
ICTA	Information and Communications Technology Authority
ID	Identifier / Identification
IEC	International Electro-technical Commission
IFMIS	Integrated Financial Management Information System
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JSON	JavaScript Object Notation
KDF	Kenya Defense Forces
KES	Kenya Shilling
KoTDA	Konza Technopolis Development Authority
KPIs	Key Performance Indicators
KSG	Kenya School of Government
1MCDAs	Ministries, Counties, Departments and Agencies
MFA	Multi-Factor Authentication
MICDE	Ministry of ICT and the Digital Economy
ML	Machine Learning
NC4	National Computer and Cybercrimes Coordination Committee
NCSS	National Cybersecurity Strategy
NSCA	National Security Council Act
OAG	Office of the Auditor-General
ODPC	Office of the Data Protection Commissioner
OpEx	Operational Expenditure
OVF	Open Virtualization Format
PaaS	Platform as a Service
PAM	Privileged Access Management
PHP	Hypertext Preprocessor
PS	Principal Secretary for ICT
PUE	Power Usage Effectiveness
RBAC	Role-Based Access Control
RDS	Relational Database Service
ROI	Return on Investment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAP	Systems, Applications, and Products (in Data Processing)

SDICT	State Department for ICT
SDICT&DE	State Department for ICT and the Digital Economy
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Centre
SQL	Structured Query Language
TCCD	Technology Change Control Document
TCCF	Technology Change Control Framework
TCO	Total Cost of Ownership
TLS	Transport Layer Security
VM	Virtual Machine
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
XML	eXtensible Markup Language

EXECUTIVE SUMMARY

Kenya's Cloud Policy (2025) Implementation Guidelines envision a secure, resilient, and interoperable cloud computing ecosystem that accelerates digital transformation, enhances public service delivery, and drives efficient use of public resources. The Guidelines position cloud computing as a foundational enabler of Kenya's digital economy, supporting sustainable development, innovation, and inclusive access to government services while safeguarding national interests.

Recognizing the strategic importance of data and digital infrastructure, the Guidelines commit to strong data sovereignty, cybersecurity, and compliance with national legal and regulatory frameworks. Cloud adoption under these Guidelines is anchored on strict adherence to existing policies, laws, and standards governing data protection, ICT governance, public finance management, and cybersecurity. These measures ensure that cloud deployment across government is secure, lawful, and accountable.

The Guidelines provide a comprehensive framework to guide public sector entities in transitioning from fragmented and high-risk ICT environments to a coordinated, cloud-first approach. They prohibit the hosting of government systems, data, and applications on personal computers, unauthorized server rooms, and unapproved entity-dedicated data centres. To ensure operational continuity and security, limited exemptions are provided for specific functions such as connectivity infrastructure, identity and access management, IoT and smart equipment, internal-use applications, and premises security systems, subject to approval by the Cloud Adoption Committee (CAC).

Developed through alignment with national digital transformation priorities and institutional oversight mechanisms, the Guidelines emphasize centralized governance and coordinated implementation. Entities operating server rooms or data centres must seek formal exemptions through the CAC, and all non-exempted systems and data must be migrated to approved cloud environments within twenty-four (24) months. The establishment of new data centres is restricted and shall only be permitted where they have been duly approved and are fully compliant with the prescribed national and international standards and certifications.

At the core of the Guidelines is Kenya's aspiration to adopt a cloud-first model across all public sector ICT investments. The National Treasury and the Ministry responsible for ICT and the Digital Economy (MICDE) are tasked with prioritizing funding for certified National Government Data Centres, consolidating budgets, and establishing financing mechanisms to accelerate cloud adoption. All cloud deployments are required to incorporate both primary and disaster recovery capabilities to enhance resilience and service continuity.

The Guidelines further underscore the importance of collaboration among key stakeholders. Government institutions will provide policy direction, funding, and oversight; the Cloud Adoption Committee will guide approvals and compliance; Cloud Service Providers will deliver secure and standards-compliant services; and public sector entities will drive implementation and service transformation. A framework agreement for Government Cloud Service Providers (GCSPs) will standardize procurement, promote economies of scale, and reduce duplication across government.

Implementation of the Kenya Cloud Policy Guidelines will follow a phased approach, beginning with foundational governance, infrastructure readiness, and funding alignment, followed by systematic migration of systems, capacity building, and continuous monitoring and evaluation. This approach ensures orderly transition, risk mitigation, and measurable progress. In conclusion, the Kenya Cloud Policy (2025) Implementation Guidelines present a strategic and coordinated roadmap for consolidating government ICT infrastructure, strengthening data security and resilience, and optimizing public expenditure through cloud adoption. The Guidelines call upon all stakeholders to collaborate in realizing a secure, efficient, and future-ready government cloud ecosystem that supports Kenya's long-term digital and socio-economic development goals.

FOREWORD

As Kenya continues its journey towards a digitally empowered society, cloud computing has emerged as a transformative force in modernising government operations, enhancing service delivery, and strengthening national digital resilience. The Government of Kenya remains committed to harnessing cloud technologies as a strategic enabler for sustainable development, economic growth, and efficient public service delivery. The development of the Kenya Cloud Policy (2025) Implementation Guidelines marks a critical milestone in advancing this commitment.

Cloud computing is a foundational technology underpinning digital government, data-driven decision-making, and innovation across the public sector. From improving access to citizen services and enabling secure data sharing to enhancing business continuity and disaster recovery, cloud technologies present significant opportunities to improve efficiency, scalability, and responsiveness. At the same time, the rapid evolution of cloud services demands a coordinated approach that safeguards data sovereignty, cybersecurity, and compliance with national legal and regulatory frameworks.

These Guidelines are not merely a technical reference for cloud adoption; they provide a strategic and governance-oriented framework to guide public sector entities in transitioning from fragmented and high-risk ICT environments to a secure, standardised, and cloud-first model. They establish clear principles, roles, and responsibilities to ensure that cloud adoption across government is deliberate, compliant, and aligned with national development priorities.

The development of the Kenya Cloud Policy (2025) Implementation Guidelines has been informed by consultations and engagements across government institutions, oversight bodies, and key stakeholders within the ICT ecosystem. This inclusive and collaborative approach reflects our shared vision for a modern, resilient, and interoperable government digital infrastructure that supports innovation while protecting the public interest.

The successful implementation of these Guidelines will require strong leadership, sustained collaboration, and disciplined execution. We therefore call upon all public sector entities, cloud service providers, and partners to work together in implementing these Guidelines, ensuring that cloud adoption delivers tangible value, strengthens public trust, and supports Kenya's long-term digital transformation agenda.

Together, we can build a secure and future-ready government cloud ecosystem that enhances service delivery, optimises public resources, and positions Kenya as a leader in digital governance and innovation on the African continent.

H.E. Hon William Kabogo Gitau,EGH
Cabinet Secretary
Ministry of Information, Communication and the Digital Economy

ACKNOWLEDGEMENT

The development of the Kenya Cloud Policy (2025) Implementation Guidelines was a collaborative effort involving a wide range of stakeholders whose commitment, expertise, and dedication were instrumental in shaping this important policy framework. On behalf of the Ministry, we extend our sincere appreciation to all individuals and institutions that contributed to this initiative.

First, we wish to acknowledge the leadership and vision of the Government of Kenya, particularly the Cabinet Secretary and senior leadership, whose steadfast commitment to digital transformation and public sector reform provided strategic direction throughout the policy development process. Their guidance and support were critical in advancing a coordinated and cloud-first approach across government.

We also extend our sincere appreciation to the members of the Cloud Adoption Committee, technical working groups, and steering committees whose expertise and tireless efforts ensured that the Guidelines are robust, secure, and aligned with national priorities. Their contributions were central to developing a comprehensive framework that addresses Kenya's unique operational, regulatory, and infrastructure needs.

We further acknowledge public sector entities, county governments, and agencies that participated in consultations and provided valuable insights on current ICT environments, challenges, and opportunities. Their practical perspectives helped shape Guidelines that are realistic, implementable, and responsive to the diverse needs of government institutions.

We are grateful to our partners from the private sector, academic institutions, and civil society organizations for their contributions throughout the consultation process. Their technical knowledge, policy insights, and constructive feedback strengthened the quality of the Guidelines and ensured alignment with industry best practices and emerging technologies. Special appreciation is extended to our international development partners for their technical and financial support, as well as for sharing global best practices and lessons learned in cloud governance, cybersecurity, and digital infrastructure transformation.

Finally, we acknowledge the Government of Kenya's continued commitment to building a secure, resilient, and future-ready digital government. The Kenya Cloud Policy (2025) Implementation Guidelines are a testament to the power of collaboration and shared purpose, and we look forward to working together with all stakeholders to ensure their successful implementation in support of efficient, secure, and citizen-centric public service delivery.

Eng. John Tanui, CBS
Principal Secretary
State Department for ICT and the Digital Economy

CHAPTER ONE: INTRODUCTION

1.1 Background

The Kenyan government recognizes the pivotal importance of Digital Transformation in cultivating a contemporary, flourishing, and inclusive society. This involves embracing emerging technologies to improve efficiency and productivity in disseminating information and services. The storage and connectivity of data play a crucial role in ensuring prompt, cost-efficient, and secure access to information. Acknowledging this, the Kenyan government intends to shift towards Cloud Infrastructure and Solution Services to supplement its traditional data storage and computing framework, thus establishing a more robust, efficient, cost-effective, and secure environment.

The Ministry of Information, Communications and the Digital Economy has been tasked with establishing digital governance frameworks for effective utilization of emerging technology. This initiative aligns with the African Union (AU) agenda 2063, Kenya Vision 2030, ICT Masterplan 2022-2032 and the Bottom-up Economic Transformation Agenda (BETA). Through this mandate the Ministry of ICT established the Kenya Cloud Policy (2025).

The Kenya Cloud Policy (2025) aims to prioritize the adoption of cloud-based information and communication technologies, covering infrastructure, hardware, software, information security, licensing, storage, data provision, as well as services such as security, development, virtualization, databases, or any other technology where cloud solutions are deemed equivalent to alternative technological solutions.

Cloud computing is increasingly recognized as a vital aspect of digital transformation and innovation. The primary definition of cloud services lies in technology, optimal cost, maturity, reliability, sustainability, performance, and enhanced security.

Innovations driven by cloud computing offer significant potential benefits, often necessitating the movement of data across international boundaries. Balancing the facilitation of seamless data flow with the imperative to safeguard privacy, individual and public safety, and national security poses a challenge.

Existing legal frameworks constrain cross-border data flows. Adoption of this policy will align with legal principles as outlined in the Data Protection Act, (2019). It is recommended that all entities adhere closely to these legal directives when determining the appropriate cloud storage locations for their data flows.

1.2 Purpose

The purpose of this policy is to:

i. Ensure the seamless transition from traditional on-premises data centre practices to Cloud Computing technology.

ii. Facilitate cross-border transmission, fostering interoperability and strengthening collaboration across nations.
iii. Complement other relevant existing cloud computing regulations.

1.3 Scope

The Kenya Cloud Policy (2025) applies to all entities operating in Kenya and any entity utilizing data residing or emanating from Kenya.

While the policy encourages widespread cloud adoption, entities may be exempted upon approval by the cloud adoption committee.

In scenarios where data may be stored or transmitted between two or more sovereign states, it is recommended that the entities comply with Data Protection Act (2019) and attendant regulations.

1.4 Rationale

The Kenya Cloud Policy (2025) is a strategic approach prioritizing cloud-based solutions over traditional on-premises infrastructure when considering new IT projects or initiatives.

The successful adoption of cloud computing technology is anticipated to yield several key outcomes:

i. **Cost savings:** Utilizing cloud infrastructure reduces expenditure on purchasing, setting up and maintenance. This streamlines technology operations and enhances service efficiency.
ii. **Service Enhancement:** Cloud solutions enable entities to seamlessly address service demands, with technology that support agility to meet requirements without interruption.
iii. **Innovation:** Cloud adoption allows for the swift and secure deployment of applications, leveraging modern technologies and frameworks.
iv. **Improved Cybersecurity:** Cloud solutions bolster resilience against cybersecurity threats, offering enhanced cybersecurity and privacy protection.
v. **Scalability:** Moving to the cloud ensures that infrastructure remains future-ready, enabling organizations to embrace the latest technologies rather than relying on outdated platforms.
vi. **Enhanced collaboration:** Cloud solutions facilitate effective collaboration by enabling easy data sharing across entities and jurisdictions fostering greater productivity and creativity in delivering online services.
vii. **Global reach:** Cross-border data transmission enables entities to expand their reach beyond local boundaries, tapping into international opportunities.

CHAPTER TWO: OVERVIEW OF CLOUD COMPUTING

Policy clauses	Implementation guidelines	Actor	Requirements
2.2 Policies and Legal Framework	While adopting the Kenya Cloud Policy (2025), entities should ensure strict adherence to all policies, legal frameworks & regulatory requirements.	CSP and data controller and data processors	Actors to familiarize themselves with the policies and legal framework requirements
2.4 Current State			
i. Personal Computers	Entities are prohibited from hosting systems, data, and applications on personal computers.	Entities as defined under the Kenya Cloud Policy (2025)	Entities to adhere to the guidelines
ii. Server rooms and data centres	Entities are prohibited from hosting systems, data, and applications in Server rooms and entity-dedicated data centres except when authorized by the Cloud Adoption Committee (CAC) Exemptions for entities to operate the data	Entities as defined under the Kenya Cloud Policy (2025), CAC	Entities should apply for exemptions to the CAC for considerations.

Policy clauses	Implementation guidelines	Actor	Requirements
Server rooms and data centres	centre or server rooms shall be processed through the Cloud Adoption Committee (CAC) Entities shall be allowed to operate owned server rooms and data centres for some selected services, like: i. Managing user access ii. Internet provision, Network/connectivity equipment, Intranet, and any other equipment that will facilitate connectivity to the cloud. iii. Function-specific equipment such IOT, Smart equipment, etc iv. Applications for internal use v. Premises security systems such as CCTV, access control systems, etc Restrict funding to only server rooms and entity dedicated data centres approved by the CAC.	Entities as defined under the Kenya Cloud Policy (2025)	Entities to adhere to the guidelines

Policy clauses	Implementation guidelines	Actor	Requirements
	Migrate the non-exempted data and systems within 24 months. Entities are restricted from establishing new data centres unless approved by the CAC. Approved Data Centres should meet defined National and International standards & Certifications.		
iii. National data centres	The National Treasury & MICDE shall prioritize adequate funding for the construction & operationalization of Certified National Government Data Centres All Entities shall prioritize cloud-first approach in all ICT Investments The government shall prioritize funding for the adoption of Kenya Cloud Policy (2025) by entities by consolidating and availing funds/budgets to drive the adoption.	The National Treasury, MICDE, entities and CAC	National Treasury and MICDE to establish a fund (to be administered under MICDE) and allocate resources for both cloud adoption and data centres infrastructure establishment.

Policy clauses	Implementation guidelines	Actor	Requirements
National data centres	Entities shall be required to have both Primary & Disaster Recovery deployment The government shall come up with a framework agreement for GCSPs		

Policy clauses	Implementation guidelines	Actor	Requirements
iv. 3rd party owned Data Centres / Cloud Services Providers:	All 3rd party owned Data Centres / Cloud Services Providers (CSPs) to the entities shall be required to meet National and International standards & certifications *(Appendix IV- framework for accreditation of cloud service providers GCSPs and non-GCSPs approval)* The Government shall enter into framework contracts with 3rd party owned Data Centres / Cloud Services Providers to provide Government Cloud Services Contractual documents shall address the code of conduct between the engaged parties Entities shall deploy only to the contracted Government Cloud Services providers for 3rd party owned Data Centres / Cloud Services Providers.	GOK Entities CSPs	MICDE to onboard 3rd Party Cloud Service Providers in adherence to standards and certifications. Government shall create a conducive ecosystem to promote investment by the 3rd Party data centres / CSP

Policy clauses	Implementation guidelines	Actor	Requirements
3rd party owned Data Centres / Cloud Services Providers	Entities shall adhere to data classification while making decisions on hosting platforms		

Policy clauses	Implementation guidelines	Actor	Requirements
2.5 Challenges:			
i. Limited resources	Limited financial & human capital may hinder Entities' ability to adopt the Cloud Policy. To overcome this: Entities shall provide sufficient resources for the training of the human capital to handle the adoption of the cloud policy Entities shall outsource professional services within the industry to fast-track migration to the cloud GCSPs shall collaborate with entities in offering capacity building	Entities GCSPs	Capacity building through training and outsourcing
ii. Security Risks	Security risks shall be addressed through the cloud service provider selection matrix adopted from both National and International standards and best practices *(Appendix III-*	Entities GCSPs	MICDE to evaluate the GCSPs against the matrix at the point of onboarding the GCSPs and throughout.

Policy clauses	Implementation guidelines	Actor	Requirements
	Accreditation framework for GCSP)		
iii. Data Silos	Authorized specific data sets shall be hosted centrally in the cloud and shall be accessible to authorized entities to facilitate data sharing, collaboration, and interoperability of the data governance strategy. (MICDE to develop)	GOK Entities, Data controllers and processors CSPs	MICDE to develop data governance frameworks *(Appendix III- Accreditation framework for GCSP)*
iv. Disaster Recovery	Entities shall have Primary & DR deployment for their data & hosted systems. Baseline standards for DR to adhere to National and International standards Entities shall be required to regularly simulate the functionality of the DR sites and submit reports to CAC – to submit annually	GOK Entities CSPs CAC	Entities align to international standards Entities to develop Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

Policy clauses	Implementation guidelines	Actor	Requirements
v. Compliance and regulatory requirements	All Entities & GCSPs shall ensure compliance with all regulatory and legal requirements. Entities shall undertake data impact assessment where required in consultation with ODPC.	GOK Entities CSPs, data processors and data controllers	Entities to adhere to all the regulatory and legal requirements
2.6 International Best Practices			
i. International Governance Framework	Entities shall identify critical data requiring local storage or sovereign cloud environment. Entities shall adhere to established conditions for foreign cloud service providers for transparency, compliance and local presence requirements Entities shall maintain control of critical national and personal data regardless of where the cloud services are provided	GOK Entities CSPs	Identify critical data requiring local storage or sovereign cloud environment.

Policy clauses	Implementation guidelines	Actor	Requirements
ii. Codes of Conduct for Responsible Use of cloud computing services:	Entities shall abide by the code of conduct that promote responsible use of cloud computing services across all sectors, ensuring ethical practices and mitigating potential risks.	GOK Entities CSPs	Entities shall adhere to the developed code of conduct CAC to provide Code of conduct *(Appendix II- contract drafting checklist – entity ↔ GCSP agreements)*
iii. Data Interoperability and Portability	Data Portability: CSPs & entities shall facilitate data portability that safeguards against potential risk such as Vendor-lock in. Data Interoperability: Entities and CSPs shall adhere to open and data interoperability standards.	GOK Entities CSPs	Compliance with open standards to be included in the data governance
iv. Global standardization	All CSPs and entities shall adhere to best global practices on cloud computing	GOK Entities	CSPs and entities adhere to the National and

Policy clauses	Implementation guidelines	Actor	Requirements
	standards as per the national and international standards.	CSPs	International standards
2.6.1 Data Location Concepts			
i. Data Localization	1. Storage location be guided by: i. DPA provisions ii. Data Classification as per the acts such as KDF act, NSCA, official secrets act or any other written law. iii. Top Secret & Secret data shall be hosted at national Government Data Centres/ private/dedicated Government Cloud located in Kenya and meeting the latest international technical, cybersecurity, and compliance standards 2. Open Data should be hosted in GCSP to facilitate innovation and international collaboration, ensuring compliance with international	ODPC Entities	ODPC to review and approve the location requests Entities to classify the data and submit to the CAC for review

Policy clauses	Implementation guidelines	Actor	Requirements
Data Localization	data protection standards.		
ii. Data Sovereignty	The contractual engagement between the CSP and entities shall provide for the Legal control, access and management of such data and systems by the data owner throughout the contractual period. The entities shall do due diligence to ensure that the CSP is able to adhere to the provisions of the data sovereignty.	CSP and entities	CSPs and the entities shall ensure adherence to the provisions of the data sovereignty.
iii. Data Residency **Data Residency**	Regardless of the data residency, the entities and the CSP shall ensure that the jurisdiction is compliant with the DPA (2019)	CSP and entities	Entities shall get clearance from ODPC to host the data outside the country

Policy clauses	Implementation guidelines	Actor	Requirements
iv. Cross-Border Data Flow	CSPs and the entities shall implement legal and technical controls to ensure compliance with Kenyan laws. There should be no cross-border data flow without the entities' written authority.	CSP and entities	CSP to initiate the request to the entities clearly indicating specific data sets. Written consent by the entities to the CSPs allowing cross border data flow on a need basis.
v. Legal Notification Framework	Due legal process must be followed before a Kenyan data is released to a foreigner	CSP, Entities Relevant Government agencies	All Entities to follow the due legal process
2.7 Cloud Services and Deployment Models			
2.7.1. Service Models	i. On premise is prohibited except for instances allowed by the Cloud Adoption Committee	Entities *GCSPs* *SDICT&DE*	The CAC to provide SLA checklist *(Appendix II-contract drafting checklist – entity ↔*

Policy clauses	Implementation guidelines	Actor	Requirements
Service Models	ii. The entities and the CSP shall abide by the SLA checklist developed by the CAC		*GCSP agreements)*
	iii. For the purposes of ensuring control and security of government data; top secret, secret and restricted shall be stored in GCSP platforms.		SDICT&DE to onboard CSP to becoming GCSPs
2.7.2 Deployment Models	Entities shall comply with the decision-making process (figure 3 in the cloud policy) in deciding the deployment model to adopt	Entities	Entities to adhere to the decision-making process
2.7.3 Cloud Service Provider Requirements	i. Location Transparency: CSPs and entities shall maintain and provide updated documentation of all data storage locations to the Cloud Adoption Committee.	CSPs, entities and CAC	CAC to provide a template for the register *(Appendix VI: location transparency template).*

Policy clauses	Implementation guidelines	Actor	Requirements
Cloud Service Provider Requirements	ii. Legal Compliance: Ensure all contracts and agreements for hosting data adhere to the Kenyan laws. Document applicable jurisdictional frameworks and any conflicts thereof. Establish clear procedures to resolve legal disputes, commercial disputes and technical disputes involving Kenyan data. Such procedures should be governed by Kenyan law. iii. Dispute resolution mechanisms: shall be clearly spelt out in the contracts.		Entities to submit the reports annually or any time there is a change. Entities to ensure that agreements, reporting tools comply legally Contracts and agreements should be clear on how disputes are resolved.

CHAPTER THREE: POLICY STATEMENT

Policy Clauses	Implementation Guidelines	Actor	Requirements
3.2 Statements	i. Cloud First. All public entities (National Government, Ministries, Counties, Departments and Agencies (MCDAs) shall prioritize cloud-based solutions when making ICT investments. Public Entities with existing cloud infrastructure shall evaluate their infrastructure for compliance with the Cloud Policy (Cybersecurity, Technical, Commercial, Data classification and Legal requirements).	Public entities, CAC	Entities shall adhere to the self-evaluation matrix CAC to provide a self-evaluation matrix *(Appendix V-cloud compliance self -evaluation matrix)* Entities to submit the assessment reports to the CAC for review, validation and recommendation.
	ii. Hosting Requirements of different Data Classifications. All entities must host data based on the following classification: a) Top Secret / Secret data – Must be hosted within Government Cloud Service Providers (GCSPs) in private/dedicated government cloud located in Kenya. If standards mentioned in section 2.1 above are	CSPs Entities CAC	MCDA's Steering Committee CAC to provide framework for accreditation of GCSPs (*Appendix IV-Framework for accreditation of cloud service providers GCSPs and non-GCSPs approval*) Entities shall use the accredited GCSPs for on-

Policy Clauses	Implementation Guidelines	Actor	Requirements
Statements	unmet, internal hosting is allowed with approval. b) Restricted data– Hosted with GCSPs in public cloud infrastructure located in Kenya (if standards are met) or internally with requisite approval. c) Open data– Must be hosted in public cloud infrastructure by GCSPs to support transparency and open governance. If Government Cloud Service Providers (GCSPs) are unable to meet the required technical, security, or commercial, standards for specific Government requirements, entities are permitted to assess and explore Third-Party Cloud Service Providers, provided these providers comply with the Kenyan data sovereignty laws, the Data Protection Act (2019) and other international regulations. The use of the third-party cloud service providers must be approved by the relevant authority, which will conduct a transparent and standardized review process to ensure	CSPs Entities CAC	boarding the workloads **MCDA's Steering Committee** CAC to provide framework for accreditation of GCSPs (*Appendix IV-Framework for accreditation of cloud service providers GCSPs and non-GCSPs approval*) Entities shall use the accredited GCSPs for on-boarding the workloads

Policy Clauses	Implementation Guidelines	Actor	Requirements
Statements	compliance with all relevant policies and regulations. Framework for assessment and approval for use of Third-Party Cloud Service Providers a) Compliance with Section 50, Computer Misuse and Cyber Crimes Act (CMCA) 2024 section and their regulations and related complimentary international laws b) Approval by the relevant authority c) Adherence to the standards mentioned in section 2.1		
	iii. Resource Optimization and Efficiency. All public entities shall: a) Use pooled government cloud service providers b) Leverage CSP expertise in cybersecurity c) Facilitate seamless data sharing across jurisdictions based on their data and security classification and requisite laws with responsible entities.	MICDE Steering Committee Entities	Steering committee All data centres infrastructural development should be coordinated through the MICDE Creation of a pool of trained experts

CHAPTER FOUR: IMPLEMENTATION AND GOVERNANCE

Policy Clause	Implementation Guidelines	Actor	Requirements
4.1 Implementation Strategy			
4.1.1 Migration Strategy	The migration roadmap should adopt the following: • Cloud First approach for all new ICT investments and technology refresh/upgrades shall be adopted • Exception shall be granted for on premise deployment subject to approval • MICDE and GCSPs shall do baseline assessment for all workloads including compute, storage, networking, end of life and data classification • Entities shall undertake process reengineering to institutionalize cloud operation • MCDAs to adequately upskill ICT officers and Users • Workloads shall be deployed in compliance with National and	MICDE MCDAs CSPs	Ministry to provide strategic framework for cloud migration Cloud migration roadmap (Appendix I-The cloud migration roadmap and phase migration timeline *)*

Policy Clause	Implementation Guidelines	Actor	Requirements
Migration Strategy	International standards on BCP • Security should be embedded at all layers of architecture		
	Phases Migration Timeline • Phase 1 (Months 1-6): Assessment and Planning - Complete workload assessment, develop migration plans, secure budgets • Phase 2 (Months 7-12): Pilot Migrations - Migrate non-critical workloads, validate processes, train teams • Phase 3 (Months 13-24): Full-Scale Migration - Migrate remaining workloads based on criticality • Phase 4 (Months 25-36): Optimization - Optimize costs, performance, and operations	CAC MICDE MCDAs	CAC to provide phased migration timeline *(Appendix I: the cloud migration roadmap and phase migration timeline)* MICDE to secure the budget Template for assessment *(Appendix I-The cloud migration roadmap and phase migration timeline)* Entities to submit migration plans aligned to phases
	Migration assessment Framework and approach	MCDAs MICDE GCSPs CAC	CAC to provide migration readiness approach 6R's

Policy Clause	Implementation Guidelines	Actor	Requirements
	• **Workload Discovery**: Complete inventory of applications, databases, servers, storage • **Dependency Mapping**: Identify dependencies between systems • **Migration Readiness**: Assess each workload using 6 R's framework (Rehost, Replatform, Refactor, Repurchase, Retire, Retain) • **TCO Analysis**: Calculate Total Cost of Ownership for current vs cloud		*(Appendix I-The cloud migration roadmap and phase migration timeline)* CAC to provide assessment templates and tools *(Appendix I-The cloud migration roadmap and phase migration timeline)* Entities to submit completed assessments for CAC review
4.1.2 Considerations for Cloud Policy			
i. Cybersecurity	Specific Security Controls: • Identity & Access Management: Multi-factor authentication (MFA) mandatory for all users, Role-based access control (RBAC), Privileged access management (PAM)	NC4 CSPs KoTDA MCDAs	NC4, ICTA and CAC to develop security control framework *(Appendix II-contract drafting checklist – entity ↔ GCSP agreements)*

Policy Clause	Implementation Guidelines	Actor	Requirements
	• Data Encryption: Data at rest encryption (AES-256), Data in transit encryption (TLS 1.2+), Key management service for encryption keys • Network Security: Virtual Private Cloud (VPC) isolation, Security groups and network ACLs, DDoS protection, Web application firewall (WAF) • Monitoring & Logging: Centralized logging (minimum 90 days retention), Security Information and Event Management (SIEM), Real-time threat detection, Automated incident response • Government Landing Zone: MCDAs should adopt one government landing zone i.e., Government owned cloud infrastructure, KONZA Cloud as the central landing zone for all government cloud workloads		Annual security audits to be done by the Ministry of ICT (MICDE) mandatory Standardized landing zone architecture

Policy Clause	Implementation Guidelines	Actor	Requirements
ii. Technical	**Specific Performance Requirements:** • Availability SLAs: Critical systems 99.99% uptime (52 min/year downtime), Essential systems 99.9% uptime (8.76 hours/year), General systems 99.5% uptime • Performance Metrics: API response time <200ms for 95% of requests, Database query response <500ms, Page load time <3 seconds • Recovery Objectives: Recovery Time Objective (RTO): Critical <1 hour, Essential <4 hours, General <24 hours. Recovery Point Objective (RPO): Critical <15 minutes, Essential <1 hour, General <24 hours Classification of incidents resolution SLAs	CAC MCDAs CSPs	CAC to publish standard SLA templates *(Appendix II- contract drafting checklist – entity ↔ GCSP agreements)* Weekly, monthly but at a minimum Quarterly SLA performance tracking to be done by the MCDAs. Annual reporting to be sent to MICDE and CAC mandatory

Policy Clause	Implementation Guidelines	Actor	Requirements
iii. Commercial	• Budget Consolidation: Consolidate cloud budgets across government and transition to centralized fund • Partner-led Framework: Leverage partnerships for capacity building, service delivery, and innovation Commercial - Cost Management (Cost Governance Framework) • Allocation of annual recurrent budget that is aligned to the capacity projection. • Cost Allocation: Implement tagging strategy for cost allocation by entity, department, and project. Monthly cost reports to finance teams and CAC • Budget Controls: Set spending alerts at 75%, 90%, and 100% of budget. Automatic resource shutdown for non-critical systems exceeding budget	National Treasury MICDE CAC MCDAs	Establish centralized cloud fund CAC to develop cost management framework Monthly cost reporting mandatory MICDE to support MCDAs on assessment of consumption as a basis of cost estimation.

Policy Clause	Implementation Guidelines	Actor	Requirements
Commercial	• Cost Optimization: Quarterly cost optimization reviews. Right-sizing recommendations for overprovisioned resources. Reserved instance planning for stable workloads Framework Agreements: Government to negotiate volume-based discounts with GCSPs. Standardized pricing across all MCDAs. Transparent cost structure with no hidden fees		

Policy Clause	Implementation Guidelines	Actor	Requirements
4.1.3 Contract Terms			
Selecting of Cloud Service Providers	All MCDAs shall select CSPs from the official Approved Government Cloud Service Providers (GCSPs) List, published and maintained by the Cloud Adoption Committee (CAC) this should follow based on data classification. Data Residency Requirements: Contracts shall state that Top Secret, Secret and Restricted data shall be hosted in either Government Owned Cloud or a GCSPs. They must be located within Kenyan territory.	MCDAs, CAC, CSPs	CAC to provide accredited list of cloud service providers MICDE to partner in supporting the procurement process
CSPs and End User Agreements	All the terms of service to be captured in the contract	MCDAs, CSPs	MCDAs and CSPs to adhere to the agreement terms.
Service Level Agreements (SLAs)	Every cloud contract shall define three levels of SLA: ● Critical – For critical and national security systems; requires 99.99% uptime,	Entities MCDAs, CAC, CSPs	These specifications are provided in the standard SLA *(Appendix II- contract drafting checklist – entity*

Policy Clause	Implementation Guidelines	Actor	Requirements
	<1hr/year downtime. ● Medium – For essential, non-critical systems; 99.9% uptime. ● General – Internal or non-sensitive systems; 99.5% uptime. Each level shall include: Support availability 24/7/365, response time, resolution time, and escalation matrix.		*↔ GCSP agreements)*
Exit Clause	All cloud contracts shall include an Exit Clause that guarantees: - Free and complete return of data in open formats (e.g., JSON, XML) - Defined transition support time (minimum 3 months) - No penalties for exit if CSP is non-compliant - Clear roles and timelines for data and service handover	Entities, CSPs	CAC to provide a Checklist of what shall be in the contract and SLA (*Appendix II- contract drafting checklist – entity ↔ GCSP agreements*)

Policy Clause	Implementation Guidelines	Actor	Requirements
Use of Open Standards	Contracts shall enforce the use of non-proprietary, open standards for all data, APIs, and software platforms to ensure portability and interoperability. Proprietary formats are disallowed unless mirrored with exportable open formats.	Entities, CAC, CSPs	CAC to provide a Checklist of what shall be in the contract and SLA *(Appendix II- contract drafting checklist – entity ↔ GCSP agreements)*
Cost Transparency	Contracts shall include a clear breakdown of service costs, including base charges, bandwidth, storage, support, and overage charges. All terms should include pricing escalation caps and renewal conditions.	Entities, CAC, CSPs	CAC to provide a checklist of what shall be in the contract and SLA *(Appendix II- contract drafting checklist – entity ↔ GCSP agreements*) Entities to adhere to the provisions of the contract and the cost management framework.
Subcontracting Rules	GCSPs shall disclose all third-party subcontractors (e.g., data centres, support providers). Contracts shall state that subcontractors must	GCSPs	Full disclosure of the contractor and compliance with the requirement on the policy

Policy Clause	Implementation Guidelines	Actor	Requirements
	also comply with the Cloud Policy.		
Jurisdiction & Dispute Resolution	All contracts shall be governed by Kenyan law, and disputes resolved under the Public Procurement and Asset Disposal Act.	GCSPs and entities	Compliance with the law
4.1.4 Skills and Capabilities			
Business Acumen	1. Develop training program that is aligned with Government Strategy and each MCDA's mandate and policy goals 2. Training program to focus on allocation of public funds, budgeting and procurement 3. Officers to get skills that will enhance strategic communication skills in order to articulate how projects can contribute to service delivery and cost efficiency	KSG CAC MCDAs, IT and HR departments	Partner with KSG, cloud service providers, and any other partners to provide the training.

Policy Clause	Implementation Guidelines	Actor	Requirements
Business Acumen	4. Officers to gain knowledge in legal and ethical frameworks such as Data Protection and cyber security laws		
Analytical skills	1. Gain knowledge in evaluating IT projects based on Public Service outcomes and cost-benefit and socio-economic impact 2. Understand how to apply project and risk management principles on technical, financial and vendor lock-in 3. Officers to have familiarity with the typical dimensions used to assess service delivery options, including: Cost (TCO, CAPEX, OPEX), Performance and Reliability (SLAs) 4. Gain Proficiency in use of Data analytic tools such	KSG CAC MCDAs IT and HR departments	Partner with KSG, cloud service providers, and any other partners to provide the training.

Policy Clause	Implementation Guidelines	Actor	Requirements
	as Excel, Power BI 5. Learn quantitative and qualitative evaluation techniques 6. Be proficient in report writing and communication skills such as data visualizations and executive summaries Understand the use of frameworks such as ITIL and COBIT		
Vendor Management	1. Skills in classifying workloads such as mission –critical, medium or general purpose 2. Skills in defining security, compliance, inter-operability and data residence needs 3. Contract negotiation skills that include data sovereignty and comply with government procurement laws 4. Skills in developing enforceable SLAs	IT heads in MCDAs Procurement officers Legal officers	Partner with KSG, cloud service providers, and any other partners to provide the training.

Policy Clause	Implementation Guidelines	Actor	Requirements
	such as Uptime targets, response/resolution time for incidents and penalties for non-compliance 5. Skills in developing data portability and exit plans 6. Dispute resolution skills		
Emerging Technologies	1. Continuous training on key emerging cloud technologies such as cloud security, containers, edge etc. 2. Officers to pursue government aligned cloud certifications e.g., AWS, Microsoft and google cloud 3. Establish hands on Projects and Sandboxes in MCDAs 4. Establish Government Cloud Communities of Practice 5. Hold regular seminars or workshops on public sector	IT heads in MCDAs Finance officers to include in budgets	Partner with KSG, cloud service providers, and any other partners to provide the training.

Policy Clause	Implementation Guidelines	Actor	Requirements
	focused cloud events		
4.1.5 Vendor Lock-in			
Portability Assurance	GCSPs must support data and service portability, allowing MCDAs to migrate services with Zero or minimal cost and no dependency. Data must be exportable in open formats (CSV, JSON, XML).	GCSPs Entities	Entities to ensure that it is enforced in the contract
Multi-Cloud Support Strategy	Cloud architecture should promote multi-cloud compatibility, so that workloads can move between vendors (e.g., AWS ↔ Azure ↔ Government Cloud) to avoid overreliance.	GCSPs Entities	Entities to ensure that it is enforced in the contract
Avoidance of Proprietary Lock-ins	Contracts shall prohibit exclusive use of proprietary APIs, formats, or tools that prevent easy switching of providers unless justified and accompanied by a dual-exit plan.	GCSPs Entities	Entities to ensure that it is enforced in the contract
Use of Open APIs	All services shall provide RESTful APIs or standard interfaces to ensure data	GCSPs Entities	Entities to ensure that it is enforced in the contract

Policy Clause	Implementation Guidelines	Actor	Requirements
	interoperability and system integration across platforms.		
Government Migration Tools	GCSPs shall develop open migration toolkits and scripts to facilitate seamless government data migration.	GCSPs Entities	Entities to ensure that it is enforced in the contract
Annual Vendor Lock-in Risk Audit	Each MCDA shall conduct an annual risk assessment for vendor lock-in (based on technology, legal, financial, or operational constraints) and submit to CAC.	GCSPs Entities	Entities to ensure that it is enforced in the contract
4.1.6 Vendor Management			
Approved Vendor Registry	Only GCSPs accredited by the CAC shall supply cloud services to government entities. Vendors must be reviewed annually for performance and compliance.	CAC Entities	CAC to provide the register of the accredited GCSPs
Prohibited Practices	Cloud contracts must ban: - Proprietary data formats without open equivalent - Anti-competitive bundling of unrelated services	Entities CSPs	Entities to enforce in the contract

Policy Clause	Implementation Guidelines	Actor	Requirements
	(e.g., forcing analytics tools with storage) - Hidden penalties for migration or termination - Exclusive clauses that lock MCDAs to a single vendor for years		
Vendor Performance Reviews	GCSPs must be evaluated quarterly against the SLA. Repeat underperformance triggers warnings and penalties.	GCSPs Entities CAC	Quarterly evaluation reports submission by the entities
Escalation and Dispute Protocols	Contracts shall define a multi-tier escalation matrix, including: - Support desk timelines - Dedicated account managers - Escalation to GCSPs and CAC if unresolved	GCSPS Entities CAC	Entities and CSPs to ensure escalation matrix is well defined Escalation to CAC through writing in case of violation.
Evaluation Roadmap	An Annual Vendor Evaluation Roadmap shall be developed and tracked using dashboards or scorecards. GCSPs shall submit improvement plans for any failed KPIs.	GCSPs Entities CAC	Entities to ensure submission of the performance quarterly reports

Policy Clause	Implementation Guidelines	Actor	Requirements
Termination Clauses	Every contract shall include a termination clause allowing MCDAs to exit in case of: - Repeated SLA breaches - Data compromise - Vendor insolvency - Policy non-compliance	Entities GCSPs	Clearly captured in the contract
Local Representation Requirement	All GCSPs shall have a local, accessible point of contact in Kenya for technical support, legal matters, and service follow-up. They must comply with the Data Protection Act 2019.	Entities GCSPs	Evidence of the GCSPs physical presence
Transparency in Partner Ecosystems	If GCSPs use resellers, the entire partner chain shall be disclosed, and accountability established through legal terms.	GCSPs Entities	Full disclosure and transparency
4.1.7 Data Classification			
Data Classification	Define an appropriate data classification framework which shall be adopted by all government entities to ensure data protection and governance.	MICDE, ODPC, CAC	MICDE to develop the data classification framework CAC to enforce the developed

Policy Clause	Implementation Guidelines	Actor	Requirements
Data Classification			data classification framework ODPC to assist entities in classifying their data.
	Institutionalize the data classification framework by providing the enabling legal status through regulation and cascade the same to all complying government entities.	MICDE CAC ODPC	MICDE to develop the data classification framework ODPC to assist entities in classifying their data.
	Implement and adopt the data classification framework applying the appropriate sensitivity levels to all data elements within their custody.	Entities	Entities to adhere to the classification framework
	Ensure that the CSP's comply with the data classification guidelines based on the data sensitivity as defined by the government agency seeking services.	Entities and CSPs	Entities to adhere to the classification framework
	Conduct regular reviews to ensure that	Entities CSPs	Entities to adhere to the

Policy Clause	Implementation Guidelines	Actor	Requirements
	the government entities and supporting CSP's are still in compliance with the classification guidelines		classification framework
4.1.8 Registration of Cloud Service Providers			
Registration of Cloud Service Providers	Provide the appropriate standards that cloud service providers wishing to offer services to government entities shall comply with. The standards need to adhere to national and international standards.	CAC/MICDE	Appropriate standards to be provided in the accreditation framework
	CAC to carry out the assessment and accreditation of CSP's wishing to offer services to government entities.	CAC/MICDE	CAC/MICDE to provide a list of accredited cloud service providers as per the assessment tool
Registration of Cloud Service Providers	CAC/MICDE to publish and maintain an updated list of accredited GCSP's that all government entities are required to engage for any services.	CAC/MICDE	CAC/MICDE to publish the list of accredited cloud service providers

Policy Clause	Implementation Guidelines	Actor	Requirements
	Ensure that only accredited GCSP's as published are engaged to offer services to government entities	Entities, Cloud Procurement Teams	CAC/ MICDE to publish the list of accredited cloud service providers
	Conduct regular reviews to ensure that all government entities are only using and deploying accredited CSP's	MICDE, CAC	CAC/MICDE to conduct regular reviews of the GCSPs

4.2 GOVERNANCE

GOVERNANCE BODY	ROLES & RESPONSIBILITIES	COMPOSITION	MEETING FREQUENCY
1. Policy Body	• Define objectives and scope of Kenya Cloud Policy • Set guidelines for Policy and publish updates • Define roles and responsibilities of entities • Update and adjust Policy when required • Develop policies to attract CSPs to invest in Kenya	MICDE Led by Cabinet Secretary	Quarterly Ad-hoc as needed Minutes to be submitted to the CS for ICT
2. Cloud Adoption	• Oversee cloud adoption across entities through	Multi-agency Committee constituted by	Bi-Monthly

GOVERNANCE BODY	ROLES & RESPONSIBILITIES	COMPOSITION	MEETING FREQUENCY
Committee (CAC) Cloud Adoption Committee (CAC)	pilots and migration support • Check cybersecurity, technical and commercial requirements • Handle accreditation of Cloud services offered to entities • Administer marketplace connecting Cloud suppliers with buyers • Ensure standards and interoperability compliance • Approve entities to host internally per Policy statements • Take inventory, classify and categorize types of data	CS for ICT: • MICDE representatives • National Treasury • ODPC representative • NC4 representative • Private sector representatives • Technical experts	Emergency sessions as required Minutes to be submitted to the CS for ICT
3. Security Body	• Issue cloud cybersecurity controls and guidelines based on existing regulations • Check compliance with cybersecurity controls • Conduct security audits and assessments of CSPs and MCDAs	National Computer and Cybercrime Coordination Committee (NC4) Other bodies tasked with Cybersecurity mandate	Bi-Monthly Incident-based meetings Minutes to be submitted to the PS for ICT

GOVERNANCE BODY	ROLES & RESPONSIBILITIES	COMPOSITION	MEETING FREQUENCY
	• Investigate security incidents and breaches • Provide security guidance and threat intelligence		
4. Cloud Service Providers (CSPs)	• Provide Cloud computing services in different forms: public, Gov-Cloud and private • Maintain compliance with all Policy requirements and standards • Submit quarterly compliance and performance reports to CAC • Participate in capacity building and training programs • Maintain local presence and support capabilities	Government CSPs (GCSPs) Third-party CSPs International and local players	Quarterly CAC meetings to review performance reports. Quarterly reporting Minutes to be submitted to the PS for ICT
5. National Data Management Office	• Manage, govern, digitize and grow national data to empower assets and capabilities • Protect personal and sensitive data by setting strategies, policies, regulations and controls	MICDE Other bodies dealing with Data governance	Quarterly Case-by-case reviews Minutes to be submitted to the PS for ICT

GOVERNANCE BODY	ROLES & RESPONSIBILITIES	COMPOSITION	MEETING FREQUENCY
	• Implement and monitor compliance with data protection requirements • Establish data classification Policy and ensure compliance • Review and approve cross-border data transfer requests		
6. Entities (MCDAs)	• Implement Cloud Policy within their organizations • Develop and submit cloud migration plans to CAC • Ensure continuous and transparent collaboration with all stakeholders • Comply with data classification and security requirements • Submit quarterly progress reports to CAC • Establish entity-level Cloud Steering Committees	All entities as defined in 'Scope of Policy': • National and County Governments • Organs of State/Public Enterprises • Data Controllers and Processors	Entity Steering Committee: Bi-monthly CAC reporting: Quarterly Minutes to be submitted to the PS for ICT

4.2.1 Governance Operational Procedures

PROCEDURE	PROCESS FLOW	TIMELINES
CSP Accreditation Process	• CSP submits accreditation application to CAC • CAC reviews application for completeness • Technical, security, and commercial assessment • On-site audit and verification • CAC decision and notification • Publication on approved CSP list	• Application review: 2 weeks • Assessment: 4 weeks • Audit: 2 weeks • Decision: 1 week **Total: 9 weeks maximum**
MCDA Cloud Migration Approval	• MCDA conducts workload assessment • MCDA develops migration plan • Submit plan to CAC for review • CAC reviews and provides feedback • MCDA revises plan if needed • CAC approves and issues migration certificate	• Assessment: 4 weeks • Plan development: 2 weeks • CAC review: 2 weeks • Revision (if needed): 1 week **Total: 9 weeks maximum**
Exemption for On-Premise Hosting	• MCDA submits exemption request with justification • Technical assessment of requirements • Security assessment and risk evaluation • Commercial assessment and TCO comparison • CAC decision with conditions if approved • Annual review of exemption status	• Request submission: 1 week • Technical assessment: 2 weeks • Security assessment: 2 weeks • Commercial assessment: 1 week • Decision: 1 week **Total: 7 weeks maximum**

PROCEDURE	PROCESS FLOW	TIMELINES
Incident Escalation	• Tier 1: CSP support desk (initial response) • Tier 2: MCDA ICT team escalation • Tier 3: CAC technical team intervention • Tier 4: NC4 for security incidents • Critical: CAC emergency session	• Tier 1 response: 4 hours • Tier 2 response: 8 hours • Tier 3 response: 24 hours • Tier 4 response: Immediate • Critical session: Within 2 hours

CHAPTER FIVE: MONITORING, EVALUATION AND REVIEW

5.1. Monitoring, and evaluation			
Guideline on Monitoring and Evaluation	a) Audits and Assessments: Entities shall conduct audits and assessments against compliance with the cloud policy and the established international standards: i. Annually conduct internal self-assessment. ii. Annually conduct external audits by relevant government authorities. iii. Conduct independent audits iv. Conduct necessary special audits in case of incidents and threats v. All audit reports shall be submitted to auditee, MICDE and CAC vi. All the reports shall enable determination of the degree of compliance with the policy for informed	MICDE Entities Internal auditors Independent auditors (Third-party auditors) OAG	The audits shall be done annually Entities shall allocate budget for the audits GCSPs shall provide International Standards Certificates. All audit reports shall be submitted to auditee, MICDE and CAC for review and actioning CSPs shall submit valid International Standards Certificates.

Guideline on Monitoring and Evaluation	decisions towards implementation of the Cloud policy. b) CSPs shall facilitate audits. c) Adherence to national and International Standards: Annual review of the GCSPs to ensure their compliance to the national and International Standards as per the accreditation matrix. d) Oversight by the IT Steering Committee: Entities IT Steering Committee shall oversee the implementation of and compliance with the cloud policy.		
5.1.1 Risk management			
Guideline on Risk Management	1. Compliance with Relevant Laws and Standards: - Ensure all cloud services comply with relevant laws, national and international standards such as the Data Protection Act	Entities CAC GSCPs	CSPs to provide valid certificates for compliance

Guideline on Risk Management	2019, CMCA 2018, NCSS 2022, MISS and ISO 31000 risk management among others.		

5.1.2 Risk mitigation			
Guideline on Risk Mitigation	a. Disaster Recovery Planning: - Entities shall ensure 1+1 deployment (primary and Secondary). Develop and implement disaster recovery plans to ensure business continuity in case of disruptions. b. Data Location and Retrieval Compliance: Ensure data is stored and is retrievable in compliance with legal and regulatory requirements. c. Legal, Regulatory, Privacy, and Security Compliance: Enforce compliance at the point of contracting.	Entities CAC CSPs Steering committees Third-party auditors	Adhere to the provision of the guidelines

Guideline on Risk Mitigation	d. Licensing Considerations: - Ensure all software and services used in the cloud are properly licensed.		
5.2 Effective date of review			
Effective date of review	Cloud policy will undergo review every 3 years or as necessary to ensure its relevance and effectiveness in addressing evolving technological and regulatory landscapes.	MICDE	MICDE to advise on when the review will be done

APPENDICES

APPENDIX I: THE CLOUD MIGRATION ROADMAP AND PHASE MIGRATION TIMELINE

Comprehensive Guide for Kenya Cloud Policy Implementation

1. REFERENCE GUIDE

STRATEGY	DESCRIPTION	WHEN TO USE	COMPLEXITY & COST
1. REHOST (Lift and Shift)	Move application as-is to cloud without changes	Quick wins, urgent migrations, apps that work well as-is	Low complexity Moderate cost Fastest option
2. REPLATFORM (Lift, Tinker & Shift)	Minor optimizations while migrating	Get some cloud benefits without full redesign	Low-Medium complexity Moderate cost Balanced approach
3. REFACTOR (Re-architect)	Redesign application to be cloud-native	Strategic apps needing scalability, performance, innovation	High complexity High cost initially Best long-term ROI
4. REPURCHASE (Replace)	Replace with SaaS or commercial off-the-shelf solution	Outdated custom apps, better commercial alternatives exist	Medium complexity Subscription cost Quick deployment

5. RETIRE	Decommission application completely	Unused, redundant, or obsolete systems	Low complexity Cost savings Risk management
6. RETAIN (Keep as-is)	Keep on premise, do not migrate	Not ready, regulatory constraints, specialized hardware	No migration effort Continued on premise costs Need CAC approval

DETAILED MIGRATION STRATEGIES

2.1 REHOST

REHOST - OVERVIEW

What It Means:

Move the application to the cloud with minimal or no changes. The application architecture, code, and data remain essentially the same, just running on cloud infrastructure instead of physical servers.

Common Approach:

- Convert physical/virtual servers to cloud virtual machines
- Migrate databases to cloud-based database servers
- Move storage to cloud storage services
- Replicate network configuration in cloud environment

KENYA PUBLIC SECTOR EXAMPLES:

1. HRIS System: Ministry's Human Resource Information System currently on Windows Server 2012 with SQL Server database. Migrate to cloud VM running the same Windows Server and SQL Server.
2. Document Management System: County government's document management system on physical servers. Move to cloud VMs maintaining existing PHP applications and MySQL databases.
3. Financial Management System (IFMIS modules): Existing oracle-based system. Rehost on cloud infrastructure with Oracle Database Cloud Service.

ADVANTAGES:

- Fastest migration path (weeks to months vs. months to years)
- Lowest initial cost and risk
- Minimal staff retraining required
- Immediate benefits: better uptime, disaster recovery, backup
- Can optimize later (after migration stabilizes)

DISADVANTAGES:

- Doesn't leverage full cloud benefits (auto-scaling, serverless, etc.)
- May not be cost-optimized (paying for cloud but not using efficiently)
- Carries forward existing technical debt and inefficiencies
- Licensing may need adjustment (BYOL or pay-as-you-go)

IDEAL CANDIDATES FOR REHOST:

- Applications nearing hardware refresh/end of support
- Systems that work well but need better infrastructure
- Non-critical applications for pilot migrations
- Applications with tight migration timelines
- Legacy systems that will be replaced in 2-3 years

2.2 REPLATFORM

REPLATFORM - OVERVIEW

What It Means:

Make targeted optimizations during migration without changing the core application architecture. This is the middle ground between rehost and refactor.

Common Optimizations:

- Migrate from self-managed database to managed database service (e.g., RDS, Azure SQL)
- Replace application server with containerized deployment
- Adopt managed caching, queuing, or messaging services
- Implement cloud-native monitoring and logging
- Use cloud load balancers instead of hardware load balancers

KENYA PUBLIC SECTOR EXAMPLES:

1. Citizen Portal: Existing citizen services portal on physical servers with PostgreSQL. Migrate application to cloud VMs BUT move database to managed PostgreSQL service for automatic backups, patching, and high availability.
2. License Management System: County licensing system currently using local file storage. Replatform to cloud with object storage (S3/Blob Storage) for better scalability and durability.
3. Payroll System: Current system with manual server patching. Move to containerized deployment with automated updates and cloud-native monitoring.

ADVANTAGES:

- Gets some cloud-native benefits without full redesign
- Reduced operational overhead (managed services)
- Better performance and reliability
- Still relatively fast (slightly longer than rehost)
- Better long-term cost efficiency than pure rehosts

DISADVANTAGES:

- Requires more planning and testing than rehost
- May need code changes for managed service integration
- Staff needs training on new cloud services
- Still doesn't unlock full cloud potential

IDEAL CANDIDATES FOR REPLATFORM:

- Applications with database-heavy workloads
- Systems where operational burden is high
- Applications needing better resilience/availability
- Modern applications already using standard components
- Systems where you want balance between speed and optimization

2.3 REFACTOR

REFACTOR - OVERVIEW

What It Means:

Significantly modify or completely redesign the application to be cloud-native, leveraging advanced cloud capabilities like serverless computing, microservices, auto-scaling, and managed services.

Common Approaches:

- Break monolithic applications into microservices
- Adopt serverless architecture (Functions as a Service)
- Implement event-driven architecture
- Use platform services (PaaS) instead of infrastructure (IaaS)
- Redesign for horizontal scalability and elasticity

KENYA PUBLIC SECTOR EXAMPLES:

1. National ID System: Redesign from monolithic application to microservices architecture for better scalability during peak periods (elections, census). Implement API gateway for integration with other government services.
2. Tax Filing System: Rebuild existing system as cloud-native application with serverless functions for tax calculations, auto-scaling for filing deadlines, and event-driven processing for refunds.
3. Health Records System: Re-architect to support real-time data sharing across counties and facilities, using cloud-native databases, API-first design, and mobile-first architecture.

ADVANTAGES:

- Maximum cloud benefits: scalability, performance, resilience
- Best long-term cost optimization (pay only for what you use)
- Future-proof architecture
- Enables innovation (AI/ML, analytics, IoT integration)
- Improved user experience and service delivery

DISADVANTAGES:

- Highest initial cost and effort
- Longest timeline (6-24 months)
- Requires significant technical expertise
- High risk if not planned properly
- May require complete code rewrite

IDEAL CANDIDATES FOR REFACTOR:

- Strategic, mission-critical applications
- Applications with highly variable demand
- Systems needing significant feature enhancements
- Citizen-facing services requiring best-in-class experience
- Applications where technical debt is unsustainable

2.4 REPURCHASE

REPURCHASE - OVERVIEW

What It Means:

Replace existing custom or legacy application with a commercial cloud-based software (usually SaaS - Software as a Service) or Commercial Off-The-Shelf (COTS) solution.

Common Scenarios:

- Replace custom email server with Microsoft 365 or Google Workspace
- Replace custom CRM with Salesforce or Dynamics 365
- Replace homegrown HR system with Workday or SAP SuccessFactors
- Replace legacy ERP with cloud-based ERP solution

KENYA PUBLIC SECTOR EXAMPLES:

1. Email System: Replace in-house email servers (Exchange, Zimbra) with Microsoft 365 Government or Google Workspace for Government. Includes email, collaboration, video conferencing.
2. Citizen Feedback System: Replace custom-built complaints system with ServiceNow Government or similar ticketing platform.
3. Project Management: Replace spreadsheet-based project tracking with Microsoft Project Online or similar PM tool.
4. Document Management: Replace aging document management system with SharePoint Online or Box for Government.

ADVANTAGES:

- Quick deployment (weeks to months)
- No development or maintenance burden
- Regular updates and new features from vendor
- Best-practice workflows already built-in
- Vendor handles security, compliance, backups
- Often better than maintaining aging custom systems

DISADVANTAGES:

- Ongoing subscription costs (OpEx vs CapEx)
- Less customization than custom-built solution
- May require process changes to fit software
- Vendor lock-in concerns
- Data migration from old system can be complex

IDEAL CANDIDATES FOR REPURCHASE:

- Commodity applications (email, office productivity)
- Outdated custom systems that are expensive to maintain
- Applications where commercial solutions are mature
- Non-differentiating business functions
- Where entity lacks expertise to build/maintain custom solution

2.5 RETIRE

RETIRE - OVERVIEW

What It Means:

Completely shut down and decommission the application. This means turning off servers, archiving data as required by law, and removing the application from service.

Why Retire?

- Application is no longer used or needed
- Functionality has been replaced by other systems
- Cost of migration exceeds value
- Redundant with other applications
- Technology is so obsolete that migration is impractical

KENYA PUBLIC SECTOR EXAMPLES:

1. Legacy Reporting System: Old reporting system that duplicates functionality now available in newer ERP systems. Archive historical reports and decommission.
2. Pilot Applications: Test or pilot systems that were never fully deployed. No migration value.
3. Superseded Systems: Old procurement system replaced by integrated IFMIS. The system is no longer used but servers are still running.
4. Abandoned Projects: Half-completed custom applications from failed projects. No users, no value.

ADVANTAGES:

- Immediate cost savings (server, license, support costs)
- Reduces security risk (fewer systems to protect)
- Simplifies IT landscape
- Frees up IT staff for more valuable work
- No migration effort or cost

CRITICAL CONSIDERATIONS:

- Verify NO users are still using the system
- Archive data per legal/regulatory retention requirements
- Document retirement decision and obtain approvals
- Communicate to all stakeholders
- Plan graceful shutdown with backup access period

IDEAL CANDIDATES FOR RETIREMENT:

- Zero or negligible usage in past 12 months
- Functionality completely duplicated elsewhere
- Legacy technology with no clear migration path
- Cost-benefit analysis clearly shows retirement is best option
- Test/development environments no longer needed

2.6 RETAIN

RETAIN - OVERVIEW

What It Means:

Make a deliberate decision to keep the application on-premise and NOT migrate to the cloud at this time. This is a strategic decision that must be approved by CAC per Kenya Cloud Policy.

Valid Reasons to Retain:

- Regulatory or data sovereignty requirements mandate on-premise
- Application requires specialized hardware not available in cloud
- Extreme latency sensitivity (millisecond-level requirements)
- Application will be retired/replaced within 12 months
- Recent major investment in on-premise infrastructure
- Application not yet ready (technical/organizational reasons)

KENYA PUBLIC SECTOR EXAMPLES:

1. National Security Systems: Intelligence and defense systems classified as Top Secret with hardware requirements that cannot be met by cloud infrastructure. Retain on-premise with annual CAC review.
2. Biometric Systems: Border control biometric matching requiring specialized hardware and millisecond response times. Retain until cloud-edge solutions mature.
3. Legacy COBOL Systems: 30-year-old mainframe system scheduled for replacement in 18 months. Not worth the migration effort. Retain until replacement.

4. Recently Upgraded Infrastructure: County just invested KES 50M in a new data centre (2024). Retain for depreciation period, plan cloud migration for 2027

IMPORTANT - POLICY REQUIREMENTS:

Per Kenya Cloud Policy Section 3.2:

- Entities MUST apply to CAC for exemption to retain on-premise
- Exemption requires clear technical, security, or regulatory justification
- CAC will conduct technical, security, and commercial assessment
- Exemptions subject to annual review
- Maximum exemption timeline: 7 weeks

ONGOING REQUIREMENTS:

- Must maintain compliance with same security standards as cloud
- Annual justification renewal required
- Quarterly reporting to CAC
- Must have documented cloud migration plan for future

IDEAL CANDIDATES FOR RETAIN:

- Top Secret / Secret classified systems
- Systems with specialized hardware dependencies
- Applications near end-of-life (< 12 months)
- Recently completed major on-premise investments
- Clear legal/regulatory prohibition on cloud hosting

3. DECISION FRAMEWORK

Selecting the appropriate migration strategy requires careful analysis across multiple dimensions. Use this framework to guide decision-making:

EVALUATION CRITERIA	BUSINESS VALUE	TECHNICAL COMPLEXITY	TIME & COST	RISK
Application criticality and usage	High usage = Refactor Medium = Replatform	Critical systems need thorough testing	Higher investment justified for critical apps	Higher stakes for critical apps

	Low = Rehost or Retire			

Age and technical debt	High debt = Refactor or Repurchase Modern = Rehost/Replatform	Legacy tech increases complexity	Refactor high initial cost but better ROI	Legacy = higher risk
Scalability requirements	High variability = Refactor Moderate = Replatform Stable = Rehost	Elasticity requires architecture changes	Auto-scaling reduces long-term costs	Design for scalability reduces risk
Compliance and data classification	Must align with Policy classification	Top Secret = may need to Retain	Compliance adds cost to any strategy	Compliance failure = high risk
Remaining useful life	Less than 1 year = Retire or Retain 1-3 years = Rehost	Short life = simpler approach	Don't over-invest in short-lived apps	Lower risk for temporary solutions

	3+ years = Refactor			
Available alternatives	Good SaaS = Repurchase Unique needs = Refactor	SaaS simpler than custom	SaaS faster and often cheaper	Proven SaaS = lower risk

3.1 Simplified Decision Tree

Use this decision tree as a starting point. Each application should still undergo full assessment.

START: Is the application still being used?

NO → RETIRE

Archive data per legal requirements and decommission.

YES, still used → Is it classified as Top Secret or Secret?

YES → RETAIN (on-premise) OR MIGRATE to Gov-Cloud

Must apply for CAC exemption to retain. If migrating, must use a dedicated Government Cloud.

NO, not classified → Will it be replaced within 12 months?

YES → RETAIN (on-premise)

No value in migration. Apply for temporary exemption.

NO, not being replaced → Is there a good SaaS alternative?

YES → REPURCHASE

Replace with a SaaS solution. Fastest path with least maintenance.

NO SaaS alternative → Is it a strategic/critical application?

YES, strategic → REFACTOR

Worth the investment to redesign for cloud-native benefits.

NO, not strategic → Does it need cloud-native features?

YES → REPLATFORM: Some optimization during migration

NO → REHOST: Quick lift-and-shift migration

PHASED MIGRATION TIMELINE

To support an orderly and risk-managed cloud transition for Ministries, Counties, Departments, and Agencies (MCDAs), a phased migration approach is recommended. Applications should be grouped into distinct waves based on their complexity, criticality, and interdependencies.

PHASE	CHARACTERISTICS	TYPICAL STRATEGIES
Phase 1 (Months 1-6)	• Simple, low-risk applications • No complex dependencies • Non-critical to operations • Build team confidence	• REHOST: Test environments • RETIRE: Unused systems • REPURCHASE: Commodity apps (email)

Phase 2 Core Systems (Months 7-18)	• Important operational systems • Moderate complexity • Some interdependencies • Build on Wave 1 learnings	• REHOST: Legacy apps • REPLATFORM: Database-heavy apps • REPURCHASE: Functional systems
Phase 3 Strategic Apps (Months 19-36)	• Mission-critical applications • High complexity • Significant dependencies • Strategic importance	• REFACTOR: Strategic systems • RETAIN: Systems requiring exemption

Phase	Timeline	Complexity Level	Risk Level	Dependencies	Approach
1	1–6 months	Low	Low	None	Rehost, Retire, Repurchase
2	7–18 months	Medium	Moderate	Some	Rehost, Replatform, Repurchase
3	19–36 months	High	High	Significant	Refactor, Retain

IMPLEMENTATION CHECKLIST BY STRATEGY

REHOST	1. Document current infrastructure (servers, storage, network) 2. Inventory all dependencies (databases, integrations, shared storage) 3. Select equivalent cloud resources (VM sizes, storage types) 4. Plan network connectivity (VPN, direct connect) 5. Execute pilot migration with non-production environment 6. Perform application testing 7. Schedule production migration (usually off-hours) 8. Execute cutover with rollback plan ready 9. Monitor for 30 days before decommissioning old infrastructure
REPLATFORM	1. Identify optimization opportunities (managed databases, storage services) 2. Assess code changes required for managed services 3. Develop proof of concept for key optimizations 4. Update application code as needed 5. Test with cloud-native services 6. Migrate data to managed services 7. Deploy application to cloud 8. Configure monitoring and alerting 9. Train operations team on new services
REFACTOR	1. Define target cloud-native architecture 2. Break down monolith into services/components 3. Design API contracts between services 4. Select cloud-native services (serverless, containers, managed databases) 5. Develop services incrementally 6. Implement CI/CD pipeline 7. Extensive testing (unit, integration, load, security) 8. Phased rollout with feature flags 9. Monitor performance and optimize

REPURCHASE	1. Define requirements and evaluation criteria 2. Research and shortlist SaaS vendors 3. Conduct vendor demos and trials 4. Evaluate TCO and contract terms 5. Plan data migration from old system 6. Configure and customize SaaS platform 7. Train users on new system 8. Execute data migration and go-live 9. Decommission old system after stabilization
RETIRE	1. Verify zero or minimal usage over past 12 months 2. Notify all stakeholders of retirement plan 3. Archive data per legal retention requirements 4. Document reasons for retirement 5. Obtain formal approval from CAC 6. Set read-only period (30-90 days) 7. Shut down systems and cancel licenses 8. Document savings achieved
RETAIN	1. Prepare detailed justification (technical, security, regulatory) 2. Complete CAC exemption application 3. Undergo technical and security assessment 4. Implement any conditions from CAC 5. Maintain compliance with security standards 6. Submit quarterly status reports 7. Develop future cloud migration plan 8. Renew exemption annually with updated justification

APPENDIX II: CONTRACT DRAFTING CHECKLIST – ENTITY ↔ GCSP AGREEMENTS

(Based on Kenya Cloud Policy Guidelines 2025)

1. Preliminary & Compliance Clauses

1.1 Statement of Compliance

The Contract MUST explicitly state compliance with:

1. Kenya Cloud Policy (2025)
2. Data Protection Act (2019)
3. Computer Misuse and Cybercrimes Act 2025(CMCA)
4. All national and international standards referenced in the policy
5. Applicable data classification laws (KDF Act, NSCA, Official Secrets Act, etc.)

1.2 Parties' Obligations

Responsibilities of:

1. The Entity (data controller/processor/owner)
2. The GCSP (data processor/service provider)

Confirmation that GCSP meets Kenyan, National, and international standards & certifications as required.

1.3 Approved Provider Requirement

The contract must confirm GCSP is officially listed in the Cloud Adoption Committee (CAC) approved Government Cloud Service Providers list.

2. Data Governance & Sovereignty

2.1 Data Classification & Hosting Location

Contract must indicate:

2.1.1 Hosting Location:

1. **Top Secret/Secret Data:** Must be hosted in a private/dedicated GCSP located within Kenyan territory
2. **Restricted Data:** Hosted in a public GCSP cloud within Kenya
3. **Open Data:** Hosted in a GCSP Public Cloud

- Where Top Secret / Secret data will be hosted (private/dedicated GCSP cloud in Kenya).
- Where Restricted data will be hosted (public GCSP cloud in Kenya).

- Where Open Data will be hosted (GCSP public cloud).
- Any foreign hosting must include:
    - ODPC approval
    - Entity consent
    - Compliance with DPA and sovereignty rules.

2.2 Data Sovereignty

GCSP must guarantee:

- Legal control & access of data always remains with the entity.
- No foreign access without due legal process.
- No cross-border transfer without written approval.

2.3 Data Portability & Interoperability

Contract must guarantee:

- Support for open standards, non-proprietary formats.
- Avoidance of vendor lock-in.
- Compatibility with national interoperability framework.

3. Security Requirements

3.1 Security Controls

Explicitly include:

- MFA, RBAC, PAM
- Encryption requirements (AES-256 at rest, TLS1.2+ in transit)
- DDoS, WAF and VPC isolation
- Monitoring, logging (90-day minimum), SIEM integration
- Threat detection & automated incident response
- Compliance with NC4 & ICT Authority security frameworks.

3.2 Annual Security Audits

- Mandatory annual MICDE audits.
- GCSP must provide access, documentation, logs.

4. Service Levels (SLAs)

4.1 SLA Classification (mandatory)

Include 3 defined levels:

- Critical – For critical and national security systems; requires 99.99% uptime, <1hr/year downtime. The service is down, corrupted, severely degraded and inoperable, impacting a significant group of users. There is no alternative or back-up available.
- Medium – For essential, non-critical systems; 99.9% uptime. Service is down, corrupted, severely degraded and inoperable, impacting a limited group of users. Back-up is available, but services are degraded.
- General – Internal or non-sensitive systems; 99.5% uptime. Service is insignificantly degraded; back-up is available with acceptable quality of service.

4.2 Performance Metrics

- API response time (<200ms 95% of requests)
- Database response (<500ms)
- RTO/RPO per classification
- Incident classification & resolution timelines
- Escalation matrix
- 24/7/365 support availability

4.3 Reporting Requirements

- Weekly, monthly, and quarterly SLA performance submissions
- Annual reporting to CAC and MICDE

4.4 Support requirements

- **Point of contact** - The SLA to provide the primary contact person for both CSP and the entity. The details to be captured include the Names, Designation/Title, email and mobile numbers.
- **Reporting and Escalation Matrix** - The SLA to provide the escalation matrix for incident management for both the CSP and the entity as per the table below.

Escalation Level	Timeline	Name	Section/Expertise	Contact Details
1st Level	**5 mins**		**Helpdesk**	
2nd level	**30 mins**		**Experts**	

3rd Level	**1 hour**		**Snr Expert**	
4th Level	**2 hours**		**CTO**	
5th Level	**6 hours**		**CEO/Director**	

Support provision - User support by the CSP shall be provided as follows

- All calls either through email or telephone should be issued with a ticket number.
- Telephone support within 5 minutes of a call requesting service
- On-site support within 30 minutes of a call requesting for service but not resolved through phone.

4.5 Exclusion List

Service levels are not applicable;

- in case of scheduled downtime
- Equipment, systems or services not included in the schedule attached to the contract.
- In case of actions or omissions by entities or their 3rd party representatives.

5. Commercial & Cost Governance

5.1 Cost Transparency Framework

Contract MUST include:

- Unit pricing (compute, storage, bandwidth, support)
- Cost escalation caps
- Renewal conditions
- No hidden fees

5.2 Budget Controls

- Spending alerts at 75%, 90%, and 100%
- Shutdown rules for non-critical workloads exceeding budget

5.3 Reserved Instances & Optimization

- Quarterly cost optimization cycles
- Right-sizing commitment

5.4 Compliance with Centralized Fund

- Acknowledgement of National Treasury/MICDE budget structures
- Use of framework agreements if applicable

6. Subcontracting & Third Parties

6.1 Disclosure of Subcontractors

GCSP must disclose:

- All third-party data centres
- Support providers
- Any subcontractor accessing/processing data

6.2 Compliance Requirement

All subcontractors must adhere to:

- Kenya Cloud Policy (2025)
- Data protection and sovereignty requirements

7. Data Residency, Cross-Border & Jurisdiction

7.1 Residency Requirements

Mandatory local hosting for Top Secret/Secret/Restricted data

7.2 Cross-Border Restrictions

No cross-border flow without:

- Written request by GCSP
- Written approval by Entity
- ODPC clearance

7.3 Legal Jurisdiction

Contract must state:

- Kenyan law is supreme
- Disputes resolved under Public Procurement & Asset Disposal Act
- Dispute-resolution mechanism (mediation/arbitration/courts)

8. Location Transparency & Registers

Contract must include:

- Complete list of all physical data locations
- Obligation for GCSP to update the CAC and entity on any changes
- Use of CAC-provided location transparency register

9. Exit Management & Termination

9.1 Mandatory Exit Clause

The Contract must guarantee:

- Free, complete return of all data in open formats (JSON, XML)
- Three (3) months minimum transition support
- No penalties for exit due to GCSP non-compliance
- Secure deletion/return confirmation
- Transfer of logs, configurations, runbooks, access keys (if applicable)

9.2 Exit Triggers

- Non-compliance with standards
- Breach of data sovereignty
- Certificate/standards lapse
- Security incident mishandling

10. Governance & Reporting

10.1 Mandatory Reporting

Contract must include:

- Annual DR simulation reports to CAC
- Annual security compliance reports
- Quarterly SLA reports
- Monthly cost reports

10.2 Continuous Compliance

Align with Kenyan national frameworks:

- BCP/DRP requirements
- Cloud Migration Strategy
- Konza Government Landing Zone architecture

11. Change Management

Contract must specify:

- Change request processes
- CAC notification requirements
- Entity approval requirements before major platform changes
- Versioning and documentation requirements

12. Capacity Building & Skills Transfer

GCSP obligations:

- Provide training to Entity ICT officers
- Include knowledge transfer plans
- Participate in government capacity-building initiatives

13. Prohibited Activities

Contract must explicitly prohibit:

- Hosting on personal computers
- Hosting in unapproved server rooms/data centres
- Unauthorized creation of new data centres
- Unauthorized cross-border data transfers

14. Appendices & Supporting Documents (Mandatory Attachments)

Ensure the contract references or attaches:

- CAC Standard SLA Checklist
- CAC Contract Checklist
- CAC Security Controls Framework
- CAC Cost Management Framework
- Migration Assessment (6R) Output
- Data Classification Register
- Location Transparency Register
- Approved GCSP Accreditation Letter

DR/BCP Requirements

Code of Conduct for Public Entities on Adopting Cloud Services

1. Purpose and Scope

This Code of Conduct establishes standards and best practices to guide public entities in the responsible adoption, management and oversight of cloud services. It ensures lawful, secure, transparent and ethical use of cloud technologies aligned with national laws, policies and public interest.

2. Guiding Principles

- **Legality:** All cloud adoption activities must comply with Kenyan laws, including the Data Protection Act, Computer Misuse and Cybercrimes Act, Public Procurement and Asset Disposal Act among others.
- **Transparency:** All entities must maintain openness in cloud service arrangements and data usage, providing clear communication to stakeholders.
- **Data Sovereignty:** Data must reside within jurisdictions compliant with Kenyan laws unless explicitly exempted, preserving national ownership and control.
- **Security by Design:** Cloud services must embed robust security controls from **inception, including encryption, access controls, and incident response.**
- **Vendor Neutrality:** Entities shall ensure that adoption decisions remain impartial and based on merit, security and value for money without undue preference to specific vendors.
- **Service Continuity:** Cloud solutions must guarantee high availability, disaster recovery, and minimal service disruption for critical public services.
- Fair Pricing

3. Responsibilities of Public Entities

- **Governance:** Entities shall establish clear governance frameworks to oversee cloud service lifecycle, compliance and risk management.
- **Location Transparency:** Primary and DR sites
- **Data Protection Impact Assessment:** Entities shall conduct thorough impact assessments before cloud adoption to identify and mitigate privacy risks.
- **Risk Registers:** Entities shall comprehensively register to track cloud-related risks with mitigation strategies and regular reviews.
- **Budget Controls & Cost Optimization**
- **Procurement:** Entities shall ensure transparent, fair and competitive procurement processes aligned with the Public Procurement and Asset Disposal Act, public procurement regulations and cloud-specific criteria.
- **Integrity and Ethical Cloud Use:** Entities shall ensure cloud services are used ethically, avoiding misuse, unauthorized access or data exploitation.

4. Standards for Cloud Service Providers

- **Security Certifications**: GCSPs must demonstrate recognized security certifications as proof of compliance.
- **Data Protection Guarantees**: Entities shall ensure contractual obligations for data privacy, protection and compliance with Kenya's Data Protection Act, 2019 are met.
- **Service Level Agreement (SLA) Requirements:** SLAs must define measurable performance metrics, uptime guarantees, and penalties for breaches as guided by the Cloud Adoption Committee Checklist.
- **Audit Support:** CSPs must facilitate independent audits and compliance verifications on request.

5. Data Classification and Handling Rules

- Entities shall classify data in accordance with the Government Data Classification Scheme and in adherence to existing data classification laws.
- Entities shall uphold data subject rights including consent, access, correction, and deletion as governed by the Data Protection Act. Entities shall evaluate cloud suitability for each data category before migration
- Entities shall avoid any misuse or exploitation of public data for unauthorized purposes.
- Entities shall promote accountability through data stewardship roles and regular compliance checks.

7. Cybersecurity Conduct

- Implement Multi-Factor Authentication (MFA) for all cloud access points.
- Adopt zero-trust security models limiting trust and access within cloud environments.
- Ensure continuous logging of access and activities, with regular audits to detect anomalies.
- Prepare and maintain incident response protocols tailored to cloud service environments.
- Report incidents to relevant authorities in a timely manner.

8. Capacity Building and Change Management

- Provide ongoing cloud skills training and awareness programs for staff.
- Facilitate knowledge transfer between vendors and internal teams.

- Document cloud processes, configurations, and compliance procedures transparently.

9. Environmental and Sustainability Conduct Prefer cloud providers with demonstrable green cloud practices and low carbon footprints.

- Promote reduced hardware waste through optimized resource utilization and cloud efficiency.

10. Exit, Transition and Continuity

- Plan for data retrieval and facility for secure deletion before contract termination.
- Ensure smooth handover procedures with minimal disruption to services.
- Maintain backup and continuity plans to support uninterrupted service during transitions.

11. Accountability and Enforcement

- Institute disciplinary measures for non-compliance with this Code, as per public sector standards.
- Apply contractual penalties for service provider breaches of agreed terms.
- Conduct regular internal and external audits to monitor adherence.

APPENDIX III. ACCREDITATION FRAMEWORK FOR GCSP TECHNICAL AND SECURITY STANDARDS APPLICABLE FOR CLOUD BASED ON DATA CATEGORIZATION

Technical & Security requirement	Item	GCSP-Top Secret & Secret	GCSP - Restricted	GCSP - Open	Non-GCSP	Remark
DATA CENTRE (DC)	**Location**	On Prem or Kenya	On Prem or Kenya	Anywhere	Anywhere	Provide location
	Ownership	GOK or Private	GOK or Private	Private	GOK or Private	Provide ownership documents
	DC Uptime	Tier III TCCD & TCCF TCCD- Tier Certification of Design Documents TCCF- Tier Certification of Constructed Facility				Certification / Standards
	DC PUE (Power Usage Effectiveness)	<=1.3				Technical
Standards	ISO 22123	yes				Information Security and Cybersecurity for Cloud
	ISO/IEC 27001 / 27002	yes				Information Security Management System

	ISO/IEC 27017	yes	Information Security in Cloud
	ISO/IEC 27018	yes	Protect Personally Identifiable Information (PII) in public cloud
	ISO/IEC 19086-4	yes	Security and Privacy in Cloud computing SLA framework
	ISO/IEC 22301	yes	Business Continuity Plan (BCP)
	ISO 20000/1	yes	Information Technology Service Management
	Open (OVF, CDMI)	yes	Technical (portability)
Legal Requirements	Data Protection Act	yes	All data processors and data controllers shall be required to register with ODPC. In the accreditation process, Entities and CSPs should meet cross-border conditions under Sec.48 of DPA in the

			instances where data/systems is to be hosted outside Kenya.
	Computer Misuse and Cybercrimes Act (CMCA) 2018	yes	Commitment to comply with CMCA
Cloud **(Minimum Technical requirements)**	Cloud WAF (Web Application Firewall)	yes	Security
	Anti-DDOS (Distributed Denial of Service)	yes	Security
	Load balance and High availability	yes	Network and Security
	Backup	yes	High reliability

APPENDIX IV: FRAMEWORK FOR ACCREDITATION OF CLOUD SERVICE PROVIDERS GCSP AND NON-GCSP APPROVAL

Following the process laid out in the Policy, the detailed requirements for a CSP to be accredited as Government Cloud Services Provider (GCSP) are as follows. Non-GCSPs, expected to be Software-as-a-Service (SaaS) providers either of non-sensitive data that can be hosted overseas or of data that is hosted as part of an overall solution (e.g. medical device that uses a Cloud to store images) will follow the same process:

1. CSP submits application to the Cloud Adoption Committee (see below for application contents)

2. Cloud Adoption Committee will review within 30 days and provide feedback either:

    i. Accepting the application without reservations
    ii. Accepting the application with recommendations for improving the Cloud Infrastructure
    iii. Requesting for further information to be submitted for further determination within 30 days of resubmission
    iv. Rejecting the application with specific reservations, upon which if they are addressed, the Committee will re-assess the application within 30 days of resubmission
    v. Rejecting the application with reasons and recommendations for the way forward

3. The CSP will receive one or more of the following accreditations:

    1. Government-owned GCSP, accredited to host Top Secret and Secret Data
    2. GCSP with local presence, accredited to host Restricted Data
    3. GCSP without local presence, accredited to host Open Data
    4. Non-GCSP, accredited as a third-party Cloud Service to host specific open data defined in the accreditation

4. The accreditation of the CSP shall be updated in the register of the accredited CSPs by the Cloud Adoption Committee and listed on Ministry of Information, Communications and The Digital Economy (MICDE) website. The CSP shall continue to follow all necessary regulations including the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations

5. The list of requirements for accreditation as a GCSPs.

a. Content Required in Application Form to be Accredited as a Government Cloud Service Provider (GCSP):

i. Provide evidence of the physical address and location(s) of the Cloud Infrastructure and key milestones of when it was built, when the equipment was installed, and the services provided.
ii. Provide evidence of the physical address and location(s) of the Disaster Recovery (DR) site and key milestones of when it was built, when the equipment was installed, and the services provided.
iii. List the services and workloads that can be delivered on the Cloud Infrastructure, including compute, storage and networking, and its architecture.
iv. Disclose partnership relating to cloud with other service/software providers and share the contractual terms related to location and storage to ensure compliance with these guidelines.
v. Provide evidence of compliance to the documentation of all the requirements stated in the guidelines document paying particular attention to those related to compliance with the DPA and CMCA Regulations and the requirements related to:
    a. **Ownership and Location**: For those applying for Government-owned GCSP and Kenya-based GCSP accreditations, information related to the applicant's ownership and physical locations of the Cloud Infrastructure will be important.
    b. **Standards and Certifications:** List the current and valid certifications achieved (ISO 27017, ISO 27018, ISO 27001, ISO 27002, ISO 27007, ISO 19086-4, ISO 22301 and any other applicable) and provide data controller and data processor registrations.
    c. **Resilience, Availability and Back-up:** provide the current performance and reliability of the Cloud Infrastructure (including Uptime certification, Service Level Availability (SLA) percentage, latency performance, redundancy and DR situation). Provide details of the DR plan.
    d. **Data Management and Data Controls:** provide the technical and non-technical measures in place to ensure data management, compliance with cross-border data requirements, and data portability/interoperability.
    e. **Local Support and Skillsets:** List staff (leadership, management and technical) who manage the Cloud Infrastructure and their qualifications, any other staff who have physical access to the infrastructure, and any staff who have administration or developer rights to access the Cloud

Infrastructure, and provide the details of the locally available point of contact and support desk system.

b. Content Required in Application Form to be Accredited as a non-GCSP Third-Party Cloud Service Provider

i. State the location(s) of the Cloud Infrastructure.
ii. List the services that are delivered on the Cloud Infrastructure and the nature of the data stored
iii. Share the standard contract the Third-Party signs with users in Kenya
iv. Provide the requirements stated in this Guidelines document paying particular attention to those related to compliance with the DPA and CMCA Regulations as well as providing details on relevant standards being followed and certifications obtained. In particular clarify:
    a. **Resilience and Availability:** State the current performance and reliability of the Cloud Infrastructure (including Uptime certification, Service Level Availability (SLA) percentage, latency performance, redundancy and DR situation).
    b. **Data Management and Data Controls:** State the technical and non-technical measures in place to ensure data management, compliance with cross-border data requirements, and data portability/interoperability.
    c. **Support:** Provide the details of the point of contact and support desk system.

APPENDIX V: CLOUD COMPLIANCE SELF -EVALUATION MATRIX.

Compliance Area	Requirement / Control	Status	Evidence / Remarks	Remediation / Action Needed	Responsible Unit / Owner
Cybersecurity	Encryption at rest & in transit				
	Identity & Access Management (IAM) with MFA and least privilege				
	Logging, Monitoring & Audit Trails for all cloud workloads				
	Segregation & Isolation of Sensitive Workloads				
	Compliance with international security standards (ISO 27001/27017/27018) and any other applicable				
	Incident Response & Breach Notification Procedures				
Technical Infrastructure	Data Residency / Hosting Location Compliance				

	Tracking & Transparency of Data Movement Across Jurisdictions				
	Backup, Redundancy & Disaster Recovery Mechanisms				
	Interoperability & Cloud Portability / Exit Strategy				
Data Classification & Governance	Data Inventory & Classification (Top Secret, Secret, Restricted, Open)				
	Mapping Classification to Cloud Hosting Model				
	Periodic Review & Reclassification of Data				
	Data Lifecycle Management & Retention Policies				
Commercial / Procurement	Use of Accredited Cloud Service Providers				
	Contract Terms on Data Sovereignty, Portability & Exit Rights				

	Cost Optimization & Cloud Commercial Efficiency				
	Cloud-by-default Compliance for New ICT Investments				
Legal & Regulatory	Compliance with Data Protection Act 2019				
Legal & Regulatory	Legal Access, Discovery & Audit Readiness				
	Data Sovereignty & Localisation Requirements				
	Regular Legal & Regulatory Reviews / Due Diligence				

APPENDIX VI: LOCATION TRANSPARENCY TEMPLATE

For Submission to the Cloud Adoption Committee

1. Entity / CSP Information

Item	Details
Name of Entity / CSP	
Ministry/Department/Agency (for entities)	
Registration / Certification (for CSPs)	
Contact Person	
Designation	
Email	
Telephone	
Date of Submission	

2. Overview of Cloud Services in Use

Service Category	Description	Deployment Model	Service Model	Start Date	End Date

3. Data Classification and Residency Details

System / Application	Data Classification	Primary Data Location	Backup / DR Location	Data Residency Compliance Status

4. Detailed Data Storage Location Inventory

4.1 Primary Storage Locations

Storage ID	Country	Region/City	Data Centre Name	Data Centre Operator	Type	Compliance

4.2 Backup and Disaster Recovery (DR) Locations

Backup ID	Country	Region/City	Data Centre Name	Data Centre Operator	Backup Frequency	DR Tier	Compliance

5. Data Flow Mapping

5.1 Narrative Description:

(Provide a clear description of how data is collected, stored, transferred, processed, and backed up across all locations.)

5.2 Diagram (Optional):

(Insert diagram or attach as annex.)

6. Data Sovereignty and Legal Considerations

Requirement	**Response**
Does any government data leave Kenya? (Yes/No)	
If yes, provide justification and legal basis	
Applicable cross-border data transfer agreements	
Mechanisms to ensure compliance with Kenyan laws	
Encryption at rest and in transit (Yes/No; describe standards)	

7. Security and Cybersecurity Controls

Control Area	**Description / Evidence Provided**	**Compliance Status**
Identity & Access Management		
Network Security & Segmentation		
Encryption Standards		

Logging & Monitoring Locations		
Incident Response Processes		
Physical Security of Data Centres		
Certifications (ISO 27001, SOC 2, etc.) and any other applicable		

8. Change Log / Updates to Data Locations

Date of Change	Description of Change	Impact Assessment	Reported By

9. Declaration and Authorization

I hereby confirm that the information provided is accurate, complete, and in compliance with the Kenya Cloud Policy (2025).

Name :
Designation :
Organization :
Signature :
Date :