THE REPUBLIC OF KENYA

DRAFT
KENYA CYBERSECURITY STRATEGY, 2025 - 2029

National Computer and Cybercrimes Coordination Committee (NC4)
Herufi House, 2nd Floor
Lt Tumbo Lane
P. O. Box 30091-00100
Nairobi, Kenya

2025

Foreword by the Cabinet Secretary, Ministry of Interior and National Administration

Hon. Onesimus Kipchumba Murkomen
Cabinet Secretary, Ministry of Interior and National Administration

The Kenyan Constitution, 2010, Chapter 4 (29) provides for Security as a fundamental right to each Kenyan. It is a basic necessity that allows for creation of a conducive environment for social economic development. The rapid ICT development has brought both benefits and security challenges in equal measure. Recognised as the 5th domain of warfare, the Cyberspace has drawn considerable attention as it has created avenues for both state and non-state actors to threaten our national security and ICT Infrastructure.

The developments and challenges faced within the Cyberspace, has made it increasingly necessary for the Government of Kenya to secure her cyberspace. In doing so, it has continued to develop and implement initiatives to strengthen the safety and resilience of our critical systems. These initiatives include policy and strategy formulation and reviews, enactments of laws and regulations, strengthening of governance structures, capacity building, increased awareness programmes and fostering private-public partnership, cooperation and collaboration.

The Ministry of Interior and National Security, reviewed the 1st National Cybersecurity Strategy, 2022 – 2027 and identified critical areas that require strategic interventions. This led to the development of this 2nd National Cybersecurity Strategy, 2025 -2029 that sets out new priority areas, goals and key interventions. This Strategy recognizes the cross-cutting nature of cyberspace and the need for coordinated and collective action from all sectors. In addition, it has introduced new critical pillars that include, incident response management to streamline government efforts in handling cyberattacks and the aspect of Artificial Intelligence (AI) and other emerging technologies to create a conducive environment for their use while taking into consideration the security challenges associated with them.

The Strategy prioritizes national security and the public safety of Kenyans online and sets the baseline measures of security for our critical information infrastructure sectors while still enumerating the role of organizations and individuals in ensuring the implementation of strategic interventions that deliver a safe cyberspace. It acknowledges that securing the cyberspace requires the collective effort of the security agencies, public sector, private sector, local and international business entities and citizens in order to realize Kenyan national goals and objectives.

I thank the great team that worked tirelessly to deliver this document and all the stakeholders and the great people of Kenya who provided input and feedback that delivered this National Cybersecurity Strategy as we aspire for a digital ecosystem that is inherently more defensible, resilient, and aligned with our objectives of creating a safe and trusted cyberspace. All are encouraged to work towards the successful implementation of this Strategy.

Signed: .....

Hon. Onesimus Kipchumba Murkomen
Cabinet Secretary
Ministry of Interior and National Administration

Message from the PS, State Department for Internal Security and Administration

Dr. Raymond Omollo, PhD, CBS
PS, State Department for Internal Security and National Administration

Security provides a conducive environment for national growth and prosperity. While ICT has had positive social economic impact, it has introduced new threats that just like other traditional threats, are a national security concern and require action to protect the fundamental freedoms and rights of Kenyans.

State and non-state adversaries are exploiting the cyberspace to commit crimes, steal information, destroy critical information infrastructure, disrupt critical services, conduct fraud and also undermine institutions. This calls for the development and implementation of cybersecurity measures to secure this vital space. This National Cybersecurity strategy provides strategic interventions that seeks to deliver a cyberspace for the people of Kenya.

This document builds on some of the key milestones already achieved. This includes the enactment of enactment of the cybercrime and data privacy laws; establishment of the National Computer and Cybercrimes Coordination Committee (NC4), as the national authority responsible for all cybersecurity matters in Kenya, and designation of Kenya critical information infrastructure (CII); formulation of the first National Cybersecurity Strategy, that has now been revised to produce this document; and the development of CMCA, 2018 regulations.

This revised National Cybersecurity Strategy, 2025 – 2029 has been developed through a comprehensive consultative process that involved key stakeholders. It then went through public participation where it was availed for scrutiny by all Kenyans and submissions received were incorporated to improve the initial drafts.

The Strategy defines nine (9) key pillars, which include: robust cybersecurity policy, legal and regulatory framework; enhancing cybersecurity governance; protection of Critical Information Infrastructure and essential services; building capacity and capabilities; mitigation against cybercrimes and risks; enhanced incidents detection, prevention and response; provides for constructive use of new and emerging technologies; foster private-public partnership, and finally promote international cooperation and collaboration.

The strategy acknowledges the pervasive nature of cyberspace and underscores the need for coordinated and collective action from all sectors. Therefore, all stakeholders are encouraged to cooperate and support the Government in creating a more secure cyberspace for social economic development.

Signed: .....

Dr. Raymond Omollo, PhD, CBS.
Principal Secretary
State Department for Internal Security and National Administration
and Chairman, National Computer and Cybercrimes Coordination Committee

Contents

List of Acronyms

AG	Attorney General
ANCA	African Network of Cybersecurity Authorities
CA	Communications Authority
CBK	Central Bank of Kenya
CC	Common Criteria
CCM	Cloud Controls Matrix
CII	Critical Information Infrastructure
CIRT	Computer Incident Response Team
CMCA	Computer Misuse and Cybercrimes Act
CoE	Council of Europe
GoK	Government of Kenya
ICT	Information, Communications and Technology
ISMS	Information Security Management System
ISO	International Standards Organisation
KICA	Kenya Information and Communications Act
KIPPRA	Kenya Institute for Public Policy, Research and Analysis
MCDAs	Ministries, Counties, Departments and Agencies
MIC&DE	Ministry of Information, Communications and The Digital Economy
MoI&NA	Ministry of Interior and National Administration
MoD	Ministry of Defence
MoE	Ministry of Education
MITI	Ministry of Investments, Trade and Industry
NESAS	Network Equipment Security Assurance Scheme
NC4	National Computer Cybercrimes and Coordination Committee
NIS	National Intelligence Service
NPS	National Police Service
NSOC	National Cybersecurity Operation Centre
PSC	Public Service Commission
SCAS	Security Assurance Specifications
SOC	Security Operation Centre

List of Figures

Executive Summary

The National Cybersecurity Strategy 2025 provides a unified and strategic direction for national cybersecurity management and the implementation of comprehensive cybersecurity measures across Kenya. Designed to safeguard both public and private sectors, this strategy merges sound governance with a robust framework of initiatives and interventions. It begins with a thorough analysis of Kenya's current cybersecurity landscape, detailing the existing policy, legal, and regulatory frameworks and highlighting the primary challenges and threats to our national cyberspace.

Vision and Mission: The strategy envisions a safe and trusted cyberspace for all Kenyans, aiming to create a secure and resilient digital environment that maximizes the benefits of a digital economy. This vision is supported by a mission to fortify our cyberspace through a coordinated and integrated approach.

Strategic Pillars: The strategy is underpinned by several critical pillars:

- **Policies, Laws, Regulations and Standards**: Developing comprehensive legal frameworks and standards that keep pace with evolving cyber threats.
- **Cybersecurity Governance**: Establishing clear leadership and accountability in cybersecurity efforts.
- **Critical Information Infrastructure Protection (CIIP)**: Safeguarding essential services and assets from cyber disruptions.
- **Cybersecurity Capability and Capacity Building**: Enhancing skills and resources to tackle cybersecurity challenges effectively.
- **Cyber Risks and Cybercrimes Management**: Addressing cyber threats and crimes through proactive measures.
- **Cyber Incident Response and Management**: Ensuring preparedness and swift response to cybersecurity incidents.
- **Artificial Intelligence and Emerging Technologies**: Leveraging artificial intelligence and emerging technologies to enhance security and national development as well as limit their use for crime and related attacks. Indeed, while artificial intelligence (AI) and emerging technologies can be used for malicious purposes, it is also a powerful weapon in the fight against cybercrime. Specifically, they have the potential to revolutionize the security landscape in a number of ways including to automate security protocols, to detect malicious activities, and to ensure adherence to cybersecurity regulatory compliance.
- **Foster Public-Private Partnership**: Fostering collaboration between government, private sector and industry to enhance cybersecurity.

- **Promote international Cooperation and Collaboration**: Promote international cooperation and collaboration to enhance information and intelligence sharing.

Implementation and Accountability: The strategy includes a detailed implementation matrix that assigns specific roles and responsibilities to various stakeholders within the cyberspace. Each role is defined with clear timelines and estimated costs for the initiatives, ensuring accountability and efficient resource allocation.

Monitoring, Evaluation and Learning: The evaluation of this Strategy will be undertaken periodically to ensure that its implementation aligns with government's agenda. A mid-term review will be conducted after three years, followed by a final review after five years, to assess progress and adapt the Strategy as needed. Learning as a process through which information generated from M&E is reflected upon and intentionally used to continuously improve the cybersecurity strategy execution, is built through emerging technologies to enable continuous real-time update.

This Strategy commits to defending the digital rights and security of the Kenyan people, empowering citizens and businesses to thrive in a globally competitive digital world.

Section 1: Introduction and Background

1.1 Background

Cyberspace is integral to the functioning of national and international systems, impacting security, trade networks, emergency services, communications, and both public and private sectors. It encompasses networks connecting various ICT infrastructures including the Internet, telecommunication networks, the Internet of Things (IoT), computer systems, and mobile communications, blending virtual spaces with human interactions through data and information. In Kenya, the significance of cyberspace aligns with traditional domains such as land, sea, air, and space, making it the 5th domain of warfare.

The rapid adoption and evolution of digital technologies, however, introduce significant vulnerabilities. These vulnerabilities expose the public, businesses, Critical Information Infrastructures (CIIs), and government agencies to cyber threats from various sources, including infrastructure sabotage, ransomware attacks, and cyber-enabled misinformation campaigns. These threats pose substantial risks to public safety, national security, and the stability of Kenya's globally connected economy.

In response, the Government of Kenya has launched numerous policy and legal initiatives to mitigate these risks. Notable among these is the enactment of the Computer Misuse and Cybercrimes Act (CMCA) 2018, serving as the cornerstone of national cybersecurity law. Additionally, the Government rolled out the National Cybersecurity Strategy 2022, which articulates a vision and key objectives for securing cyberspace, organized around six (6) foundational pillars namely, Cybersecurity Governance; Cybersecurity Policies, Laws, Regulations, and Standards; Critical Information Infrastructure Protection (CIIP); Cybersecurity Capabilities and Capacity Building; Cyber Risks and Cybercrimes Management; and Cooperation and Collaboration. Arising from the developments and the many cyber incidents experienced within the cyberspace, this review seeks to enhance these pillars and introduces three (3) more namely: Cyber incident response and management; new and emerging technologies; and international cooperation and collaboration.

Kenya has also introduced the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024. These regulations aim to streamline cybersecurity efforts by establishing a National Cybersecurity Operation Centre (NSOC), sector-specific Cybersecurity Operation Centres (SOCs), and a dedicated Operation Centre for Critical Information Infrastructures (CII-SOC). They also enhance the reporting mechanisms for cybercrimes through the establishment of cybercrime desks at police stations.

1.2 Cybersecurity Landscape

The expansion of Kenya's cyberspace has presented new economic opportunities and security challenges. Cybersecurity is recognized as a critical national economic and security issue and the 5th domain of warfare in addition to the traditional domains, land, air, maritime and space. Key

challenges include the exploitation of vulnerabilities by adversaries, leading to potential disruptions in critical infrastructure operations. Most ICT systems in Kenya seem to prioritize efficiency, cost, and convenience over security, often overlooking critical vulnerabilities that could be exploited by malicious actors.

The landscape is further complicated by threats such as cyber espionage, which aims to access sensitive or classified information for financial, political, or strategic gains. As ICT systems become increasingly interconnected, they are more vulnerable to sabotage, disruption, or destruction. Additionally, the spread of misinformation and fake news can undermine public trust in government and institutions, posing a direct threat to national stability. Cybercrime also continues to evolve, with an increase in incidents related to cyber fraud, including banking fraud, SIM swap scams, online Ponzi schemes, and digital extortion.

To effectively address these emerging risks and maintain cyberspace security, continuous review and updating of policies and laws are necessary. This proactive approach will enable Kenya to safeguard its digital environment, ensuring a secure and resilient cyberspace for all Kenyans.

Figure 1: Threats and Actors

Government and Stakeholder Responsibilities

In response to the challenges and threats identified, the Government of Kenya (GoK) will take the lead in defending its cyberspace to safeguard citizens and the national economy from potential harm. It will also develop both domestic and international frameworks aimed at protecting national interests, securing fundamental rights, and prosecuting cyber offenders.

Critical Information Infrastructure (CII) owners and operators, along with businesses and organizations in Kenya, are required to implement measures to protect their systems and services. These measures should include adopting a risk-based approach to cybersecurity, managing cybersecurity risks presented by vendors, adhering to minimum cybersecurity baseline standards, and actively supporting the government by reporting and responding to cybersecurity incidents.

Moreover, Kenyan citizens and non-citizens alike must take proactive steps to protect themselves and their assets in the digital realm, similar to precautions taken in the physical world. This includes safeguarding hardware such as phones and computers, as well as the data, software, and systems that facilitate personal and professional activities.

1.3 Rationale for National Cybersecurity Strategy 2022 Review

The review of the National Cybersecurity Strategy 2022 - 2027, is driven by the need to align with the Government's digital transformation agenda, ensure a harmonized approach to cyber incident response and management, incorporate artificial intelligence and other emerging technologies as well incorporate the provisions of the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024. These initiatives reflect the dynamic nature of the cyber environment and underscore the essential need for a comprehensive and adaptive strategy to protect Kenya's digital infrastructure and support its digital growth.

1.4 National Cybersecurity Strategy 2025 Development and Implementation Process

The development of the Kenya Cybersecurity Strategy 2025 - 2029, followed a five-phase approach consistent with Kenya's public policy formulation practices and international standards. The process began with the initiation phase, where a Cybersecurity Strategy Steering Committee was formed - to establish a detailed work plan. This plan outlined the major steps and activities, identified key stakeholders, and specified the timelines, human resources, and financial resources required.

During the stocking and analysis phase, data was gathered on the national cybersecurity capacity and risk landscape, which informed the drafting of the strategy. The production phase involved multiple meetings and multi-stakeholder workshops that culminated in the formulation of this strategy.

The implementation phase engages multiple stakeholders to support the execution of the strategy's identified initiatives. Finally, the Monitoring and Evaluation phase, entails periodic review to ensure that the Strategy's implementation is aligned with national goals and objectives.

Section 2: Strategic Foundations

2.1 Guiding Principles

The guiding principles of the National Cybersecurity Strategy 2025 - 2029 are derived from the objectives outlined in the Computer Misuse and Cybercrimes Act, 2018, ensuring that the strategy is robust and comprehensive. These principles are:

- **Protecting Confidentiality, Integrity, and Availability**: Ensuring that computer systems, programs, and data are secure from unauthorized access and damages.
- **Preventing Unlawful Use of Computer Systems**: Deterring the misuse of digital resources and technologies for illegal activities.
- **Facilitating Crime Prevention and Enforcement**: Aiding in the prevention, detection, investigation, prosecution, and punishment of cybercrimes.
- **Upholding Constitutional Rights**: Safeguarding the rights to privacy, freedom of expression, and access to information as guaranteed under the Constitution of Kenya 2010.
- **Encouraging International Cooperation**: Enhancing global collaboration on cybersecurity matters to address international cyber threats and crimes effectively.

These principles are further informed by Kenya's public strategy formulation process and adherence to international best practices.

2.2 Vision

Safe and Trusted Cyberspace for the People of Kenya. This vision articulates a commitment to creating a secure environment where digital interactions are protected and reliable.

2.3 Mission

To Build a Secure and Resilient Cyberspace through a Coordinated Approach while Maximizing the benefits of a Digital Economy. The mission focuses on comprehensive security measures that not only protect cyberspace but also support the growth and opportunities of the digital economy in Kenya.

2.4 Strategy Goals

The goals of the National Cybersecurity Strategy are:

1. **Strengthening Legal Frameworks**: To fortify policies, laws, regulations and cybersecurity codes and technical standards.

2. **Enhancing Kenya's Cybersecurity Governance and Institutional Framework**: To improve governance and coordination in cybersecurity efforts.

3. **Protecting Critical Information Infrastructures**: To boost the resilience and security of vital digital and physical infrastructures.

4. **Building Cybersecurity Capacity and Capabilities**: To enhance the skills and capacities necessary to address and mitigate cyber threats.

5. **Minimizing Cyber Risks and Cybercrimes**: To reduce the prevalence and impact of cyber risks and crimes through proactive measures.

6. **Streamlining Incident Response and management**: To optimize processes for responding to and managing cyber incidents.

7. **Guiding on New and Emerging Technologies**: To provide strategic oversight on the implications of artificial intelligence and other new technologies in the realm of cybersecurity.

8. **Enhancing Private-Public partnership**: To foster stronger partnerships and cooperation between the public and private sectors in cybersecurity initiatives.

9. **Promote International Cooperation and Collaboration**: To Promote global cooperation and collaboration on cybersecurity matters to address international cyber threats and crimes effectively.

2.5 Strategy Pillars

The strategy is structured around the following pillars, each essential to the holistic cybersecurity framework:

1. **Cybersecurity Policies, Laws, Regulations and Standards**: Creating and maintaining robust legal and regulatory frameworks.

2. **Cybersecurity Governance**: Establishing clear and effective leadership and administrative structures.

3. **Critical Information Infrastructure Protection (CIIP)**: Securing infrastructures essential to national security and economic stability.

4. **Cybersecurity Capability and Capacity Building**: Developing the necessary skills and technologies to enhance cybersecurity.

5. **Cyber Risks and Cybercrimes Management**: Managing and mitigating cyber threats and criminal activities.

6. **Cyber Incident Response and Management**: Responding to and recovering from cybersecurity incidents efficiently.

7. **New and Emerging Technologies**: Addressing the security challenges presented by AI and emerging digital technologies. Some of these challenges include automated creation of sophisticated attacks; creation of autonomous and self-learning malware; automated vulnerability exploitation; and Automated phishing and social engineering. However, AI and emerging technologies present opportunities that can be leveraged to enhance cybersecurity measures, automate security protocols, detect malicious activities, response and adherence to cybersecurity regulatory compliance.

   Automated creation of sophisticated attacks, Creation of autonomous and self-learning malware; Automated vulnerability exploitation; Automated phishing and social engineering

8. **Public Private Partnership:** Leveraging collective expertise and resources from both public and private sectors to enhance cybersecurity.

9. **International Cooperation and Collaboration**: Recognising that cyberthreats are cross cutting and transcends international boundaries, this policy promotes international information and intelligence to address international cyber threats and crimes effectively.

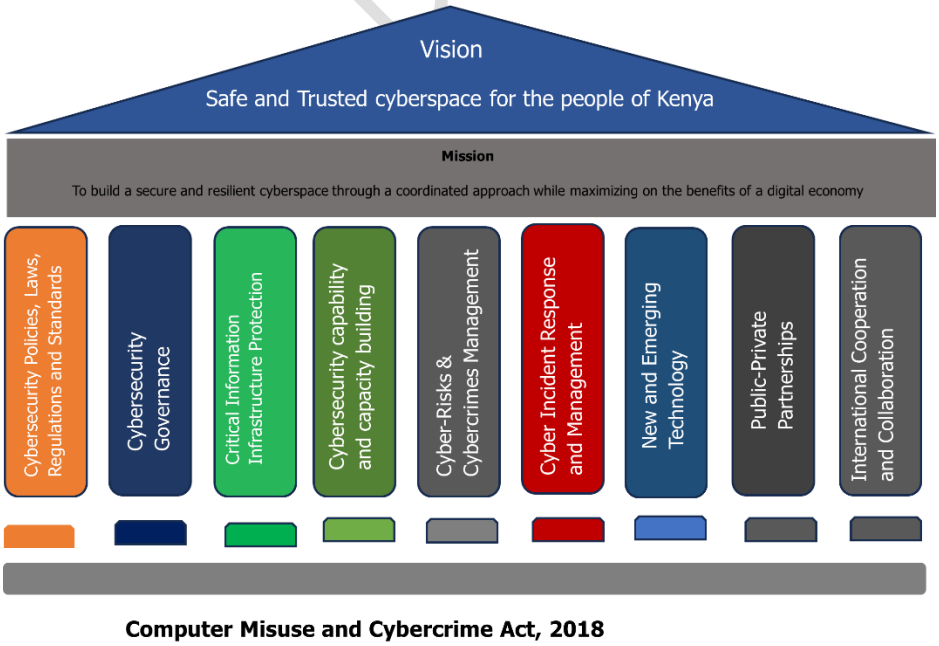

Figure 2: Kenya Cybersecurity Strategy Foundation

Section 3: Areas of Strategic Focus

3.1 Cybersecurity Policies, Laws, Regulations and Standards

The development of a safe, secure, and resilient cyberspace ecosystem hinges on a robust policy, legal, and regulatory framework. This framework is crucial for protecting information assets within Kenya, as illustrated in Figure 3, which outlines the key components and their interrelationships in the design and implementation of an Information Security Management System (ISMS).

Goal:	**To strengthen cybersecurity policies, laws, regulations and standards.**	
Objective:	To maintain up-to-date and effective cybersecurity policies, laws, regulations and standards that respond to the evolving cyber landscape.	
Interventions:	(a)	Amend the CMCA, 2018 to establish National Cybersecurity Agency and the National Cybersecurity Academy.
	(b)	Review existing cybersecurity policies, laws, regulations and standards to identify gaps and areas for improvement, as well as align with global best practices and address new cyber threats.
	(c)	Promote the implementation of the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024, to ensure a cohesive approach to managing cyber risks and crimes.
	(d)	Ratify and adopt regional, international cybersecurity conventions, treaties, laws and norms.
	(e)	Develop cybersecurity guidelines for individuals, SMEs, Large enterprises and sector specific.
	(f)	Enforce the adoption of cybersecurity codes and standards by government entities, gazetted CIIs and the private sector.
Outcome:	A coherent and effective framework of cybersecurity policies, laws, regulations, and standards that safeguards Kenya's information assets and promotes resilience against cyber threats.	

3.2 Cybersecurity Governance

Cybersecurity governance is pivotal in developing a robust cyber ecosystem essential for a thriving digital economy. Strengthening Kenya's cybersecurity governance establishes a solid foundation for safeguarding the nation against cyber threats. This pillar provides strategic direction on the governance structures and resources necessary to support the development and implementation of a secure national cyber ecosystem.

Goal:	**To enhance Kenya's institutional framework for cybersecurity governance and coordination.**

Objective:	To improve governance, resource allocation, and coordination of cybersecurity initiatives across Kenya.	
Interventions:	(a)	Establish a National Cybersecurity Agency (NCSA), a body corporate to oversee and coordinate national cybersecurity efforts.
	(b)	Assign the proposed NCSA with a dedicated budget, human capacity, infrastructure, and tools to effectively support and implement its mandate.
	(c)	Establish the National Cybersecurity Operation Centre (NSOC) to monitor, detect and prevent cyber threats and respond to cyber incidents.
	(d)	Establish and enhance Cybersecurity Operation Centers (SOC) in sectors and CIIs to manage sector-specific cybersecurity challenges.
	(e)	Establish a National Cybersecurity Academy to undertake capacity building, training, certifications of cybersecurity as well as undertake cybersecurity innovation, research and development.
	(f)	Develop a SOC Maturity Model template for the National, Sector and CII SOCs setup based on best practices.
	(g)	Establish and enhance specialized cybersecurity units within the Law enforcement agencies, Public Prosecutions, and Judiciary to handle cybercrime effectively.
Outcome:	Effective governance and coordination of cybersecurity initiatives throughout Kenya, ensuring a unified and responsive approach to emerging cyber threats	

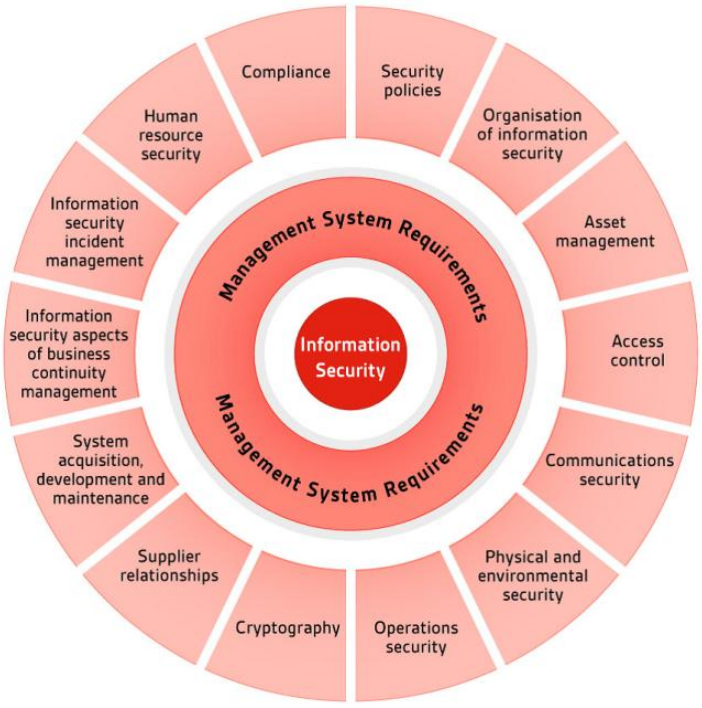

Figure 3: Information Security Management
Source: ISMS Alliance

3.3 Critical Information Infrastructure Protection (CIIP)

As digitalization progresses, Critical Information Infrastructures (CIIs) across various sectors, previously isolated, are increasingly interconnected with other digital systems. This connectivity exposes them to heightened cyber threats, thereby posing risks to national security and public safety. The Kenyan government is dedicated to strengthening the cybersecurity posture and resilience of CIIs and other digital systems and infrastructures.

Goal:	**To enhance the protection and resilience of CIIs**	
Objective:	To protect and safeguard CIIs from cyber threats and ensure their continuous operation	
Interventions:	(a)	**Operationalize the Critical Information Infrastructure Protection Framework**: Implement a comprehensive strategy for protecting CIIs that includes risk assessments and mitigation strategies.
	(b)	**Develop CII designation guidelines**: To allow for Continuously Identifying and Designating CIIs.
	(c)	Develop a National Assets inventory for all CIIs.
	(d)	**Implement Cryptography and Access Control Measures**: Secure sensitive government information and data through advanced cryptographic techniques and strict access controls.
	(e)	**Implement Baseline Cybersecurity Measures**: Establish physical and technical security controls, including emergency and disaster contingency and recovery plans, to enhance the resilience of CIIs.
	(f)	**Develop a cyber-resilience plan:** To incorporate in-country multi-data centers clustering.
	(g)	**Elevate the local Internet exchange points to an international exchange point:** This will promote the Internet Exchange Point locally.
	(h)	Develop a National repository for all Vulnerabilities.
	(i)	**Establish an Information Sharing, Reporting and Incident Response Framework**: Create a robust framework for sharing cybersecurity information, reporting incidents, and coordinating responses to enhance the overall security landscape of CIIs.
Outcome:	Increased protection and resilience of CIIs, ensuring their robustness against cyber threats and their critical role in national security and public safety.	

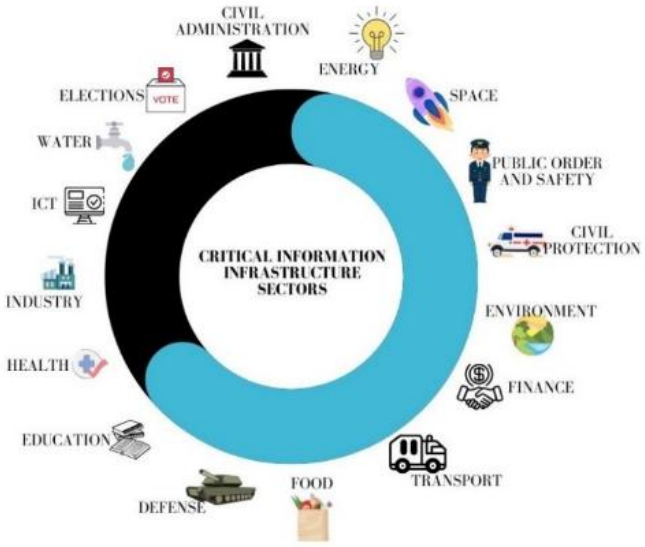

Figure 4: The sixteen Sectors of Kenya's Critical Information Infrastructures

3.4 Cyber Incident Response and Management

In our increasingly digital world, the resilience of critical systems against cyber threats is paramount. Effective robust mechanisms to ensure cybersecurity emergency readiness and response capabilities are essential to manage both minor and significant cybersecurity incidents promptly and efficiently.

Goal:	Build cyber incident response and management mechanisms to ensure effective response to cyberattacks and incidents.
Objective:	To build and enhance comprehensive incident response and management capabilities.
Interventions:	(a) **Build Cybersecurity Incident Response Teams**: Constitute cyber-incident response teams at the national and sector levels to coordinate incident response activities. Teams to be under the National Cybersecurity Agency and Sector regulators. (b) **Build Capacity to Detect Attacks and Identify Incidents**: Develop systems and processes to quickly detect and accurately identify cybersecurity incidents. (c) **Develop a Framework for Joint Incident Response**: Implement a structured approach allowing collaboration between various stakeholders in responding to cyber incidents. (d) **Formulate an Incident Response and Management Plan**: Define and set up procedures and protocols for effective cyber incident response and management. (e) **Continuous Assessment and Enrichment of Incident Response Capabilities**: Regularly evaluate and enhance the mechanisms for incident response to adapt to evolving cyber threats. (f) **Centralized Reporting of Cybersecurity Incidents**: Implement a unified system for reporting and tracking cybersecurity incidents to streamline response efforts.
Outcome:	Enhanced capability to effectively respond to cyberattacks and incidents, minimizing their impact on national security and public safety.

3.5 Cybersecurity Capability and Capacity Building

As technology evolves, so do the complexities and sophistication of cyber threats. To maintain cutting-edge capabilities and adapt to rapid technological changes, the Kenyan Government is committed to supporting advanced research, fostering local digital innovation, and developing local cybersecurity skills. These efforts are aimed **at positioning Kenya as a leader in cybersecurity on the continent. The growing need for qualified cybersecurity** professionals represents a significant and expanding opportunity within the sector. In response, the Government will collaborate with academia, research institutions, and the private sector to create new opportunities, drive investment, and foster leading-edge research and development in cybersecurity.

3.4.1 Cybersecurity Capability

Goal:	To strengthen cybersecurity capability.
Objective:	To enhance cybersecurity protection and resilience across Kenya.
Interventions:	(a) **Implement Comprehensive Cybersecurity Measures**: Deploy advanced cybersecurity protection, detection, analysis, and response tools and systems to robustly defend Kenya's digital environment. (b) **Promote Local cybersecurity innovation, research and development**: Encourage research and development of secure, competitive, cost-effective, and tailor-made cybersecurity solutions within the country. (c) **Promote Kenyan Cybersecurity firms and solutions**: Encourage use of locally developed cybersecurity solutions and joint partnership between international firms and local firms during tendering for skill and technological transfer as well as localisation of cybersecurity support.
Outcome:	Enhanced cyber protection and improved resilience against cybersecurity threats and incidents, ensuring that Kenya remains at the forefront of cybersecurity advancements.

3.4.2 Cybersecurity Capacity

Goal:	To develop cybersecurity capacity
Objective:	To increase cybersecurity expertise, education, research and awareness across the nation.
Interventions:	(a) **Operationalise the National Cybersecurity Academy**: Create an institution dedicated to training and certification cybersecurity professionals and undertaking of Cybersecurity innovation, research and development. (b) **Establish a cybersecurity think tank and/or policy institute**: with a focus on advocacy on cybersecurity and impact assessment of the cybersecurity legal and regulatory frameworks. (c) **Establish a Cybersecurity Professional Certification Program**: Develop a certification, accreditation, and career progression framework to standardize and recognize cybersecurity expertise. (d) **Develop and Implement a Cybersecurity Basic Education Curriculum**: Introduce cybersecurity education at various levels of the educational system to build a foundational understanding from an early age. (e) **Develop and Implement a Cybersecurity Awareness Raising Programme**: Launch initiatives to increase public awareness about cybersecurity risks and safe practices. (f) **Develop cyber diplomacy capacity**: Define Conduct of affairs in the cyberspace for stakeholders to safeguard interests and promote goodwill for peaceful relationships.
Outcome:	Increased cybersecurity capacity and improved cybersecurity culture, enhancing the overall security posture of the nation.

3.6 New and Emerging Technologies

The rapid advancement of technology presents both significant opportunities for progress and new cybersecurity challenges. Malicious actors exploit vulnerabilities in new and emerging technologies to disrupt infrastructure, compromise data, and undermine security. To counter these threats, the national cybersecurity strategy must continuously evolve.

Goal:	To proactively identify and mitigate cybersecurity risks associated with new and emerging technologies.
Objective:	To establish a robust cybersecurity framework capable of safeguarding national security interests against emerging threats.
Interventions:	(a) **Identify and Prioritize Cybersecurity Risks**: Focus on new and emerging technologies to understand and prioritize associated risks. (b) **Develop Risk Management Frameworks**: Create methodologies to assess and mitigate risks associated with the adoption and use of emerging technologies. (c) **Invest in Research and Development**: Support local capabilities in new and emerging technologies through funding academic institutions, industry partnerships, and public-private-led research programs. (d) **Engage in Local and International Cooperation**: Participate in multilateral efforts to develop common standards, solutions, and norms for cybersecurity in the context of emerging technologies. (e) **Invest in Workforce Development**: Address the shortage of cybersecurity professionals with training programs, educational partnerships, and skill-building initiatives. (f) **Establish Regulatory Frameworks and Standards**: Enact laws and regulations that govern the development, deployment, and use of new and emerging technologies, focusing on security-by-design, data protection, and accountability. (g) **Use new and emerging technologies** to undertake the following: (1) Automate security protocols, (2) Detect malicious activities, and (3) Ensure adherence to cybersecurity regulatory compliance.
Outcome:	A comprehensive cybersecurity framework that effectively safeguards national interests against the threats posed by AI and other emerging technologies, ensuring secure technological adoption and resilience.

3.7 Cyber Risks and Cybercrimes Management

With the increasing number and complexity of cyber threats, including malicious attacks, there is a critical need to enhance detection and remediation capabilities. Strengthening these capabilities is essential to protect, detect, respond to, and recover from cyber incidents effectively.

Goal:	To minimize cybersecurity risks and combat cybercrimes effectively.
Objective:	To mitigate cybersecurity risks and effectively manage and combat cybercrimes.
Interventions:	(a) **Develop and Implement a National Cybersecurity Risks Management Framework**: Establish guidelines for identifying, assessing, and mitigating cybersecurity risks. (b) **Perform National Cybersecurity Risk Assessments and Audits**: Regularly evaluate and audit cybersecurity practices and infrastructures to identify vulnerabilities. (c) **Develop and Implement a National Framework for Cybercrime Management**: Create a comprehensive strategy for preventing, detecting, and responding to cybercrimes. (d) **Establish a National Cybercrimes Alert and Warning System**: Set up a system to alert the public and stakeholders about emerging cyber threats. (e) **Develop Online Cybercrimes Reporting Platforms**: Create platforms for citizens and CIIs to report cybercrimes easily and securely. (f) **Operationalise Cybercrime Desks**: Provide dedicated resources at police stations to handle cybercrime reports and responses.
Outcome:	Reduced cybersecurity risks and a significant decrease in the prevalence and impact of cybercrimes.

3.8 Public Private Partnership

Cyber threats require involvement of all the stakeholders, key among them being the critical private sector players. Strengthening engagement with them is critical for securing a resilient cyberspace. The Kenyan Government is committed to working with internal stakeholders such as academia, research institutions, and the private sector to enhance Kenya's cybersecurity posture.

Goal:	To foster public-private partnership that will deliver a secure national cyberspace.
Objective:	To enhance the effectiveness of public-private partnerships and strengthen both national and international cooperation and collaboration in cybersecurity.
Interventions:	(a) **Develop a Framework for Public-Private Partnerships**: Create structures for collaboration in training, research, innovation, and information sharing among various sectors. (b) **Establish a Trusted Information Sharing Mechanism**: Implement a secure platform for information exchange and incident reporting among national and international stakeholders. (c) **Participate in Multi-Stakeholder Fora:** Actively participate in local and international fora such as CoE, Europol, ANCA, MCKB amongst others
Outcome:	Increased effectiveness and efficiency in cybersecurity partnership achieved through a unified approach that leverages strengths across public and private sectors.

3.9 International Cooperation and Collaboration

Cyber threats are inherently cross-cutting and transnational, demanding cooperation and collaboration at international levels. Strengthening engagement with international partners to

develop effective mechanisms and policies, and to implement cybersecurity initiatives, is critical for securing a resilient cyberspace. The Kenyan Government is committed to working with international partners, to enhance Kenya's cybersecurity posture.

Goal:	To promote international cooperation and collaboration in order to improve national cybersecurity posture.
Objective:	To enhance the effectiveness of international cooperation and collaboration and strengthen information and intelligence sharing in cybersecurity.
Interventions:	(d) **Develop a Framework for Regional, International Cooperation and Collaboration**: Establish guidelines and protocols that facilitate effective collaboration across different levels and borders. (e) **Participate and Promote International Cybersecurity Efforts**: Engage actively in the development and implementation of international laws, agreements, treaties, policies, norms, standards, and participate in relevant conferences and fora on cybersecurity.
Outcome:	Increased effectiveness and efficiency in cybersecurity cooperation and collaboration across borders with like-minded international partners.

Section 4: Sustainability Considerations

4.1 The Guiding Principles

Sustainability is the approach that creates long-term value for all stakeholders by embracing opportunities and managing risks. This strategy document will be made sustainable to meet the needs of the present stakeholders without compromising the ability to meet the needs of future stakeholders and or stakeholders currently unforeseen due to the very nature of dynamism in emerging technologies.

4.2 Engagement with Stakeholders for Sustainability

4.2.1 Informing/updating stakeholders

Provide basic information and updates to the stakeholders about the policy document and or a decision to keep them informed.

4.2.2 Consulting stakeholders

Actively seek stakeholder feedback, opinions, and suggestions. Provide opportunities for stakeholders to express their views by asking for their input, and consider their perspectives in the decision-making process. Consider the following:

- **Discussion forums**. Set up online discussion forums for stakeholders to participate and ask questions or respond to current issues.
- **Surveys & questionnaires**. Use E-polls, questionnaires and surveys to gauge stakeholder reactions to changes in the subject matter at all times.

- **Public hearings**. In-person meetings, such as town hall meetings and public hearings to provide a chance for stakeholders to engage and have their views heard.

- **Consultancies and Engagements with Subject Mater Specialists**. Direct engagement with consultants and subject matter specialists to take on board new and emerging technologies.

4.2.3 Involving stakeholders

Involve the stakeholders in the decision-making process. These are stakeholders who are seen as partners rather than mere recipients of information and are given the opportunity to provide input and influence the outcome. They are recognised as having valuable knowledge, experiences, and perspectives that can significantly enhance the policy.

There is an emphasis on building trust, mutual respect, and shared responsibility between the organisation and them by involving them in brainstorming, problem-solving, and generating ideas.

4.2.4 Collaborating with stakeholders

These are the stakeholders with high levels of interest, commitment and influence in the subject matter. They are active partners in decision-making, and their input is given equal weight alongside other factors. They will participate in shaping the policy or decision and share a sense of ownership. The communication channels for the stakeholders will include multi-stakeholder forums, joint planning sessions, facilitated workshops, strategic dialogues, and ongoing collaborative platforms.

4.3 Monitoring and Evaluation(M&E)

Monitoring and Evaluation of this Strategy is integrated with the National Integrated Monitoring and Evaluation System (NIMES) in order to maintain clear linkages between the implementation of this Strategy and the Vision 2030. A mid-term review of this Strategy will be conducted after three (3) years and a final review after five (5) years. In addition to these reviews, NC4 Secretariat will carry out an annual monitoring and evaluation exercise and report on the implementation of the Strategy.

Section 5: Implementation Framework

5.1 Strategy Implementation

Implementation of the Kenya Cybersecurity Strategy 2024 will adopt a multi-stakeholder approach. All the stakeholders in the Republic of Kenya shall have responsibility of establishing respective governance structures with allocation of resources including budget, human resource and infrastructure to support the overall mission of this Strategy.

NATIONAL COMPUTER AND CYBERCRIMES COORDINATION COMMITTEE (NC4) STAFF
+254-20 3230 100 | info@nc4.go.ke | www.nc4.go.ke Herufi House, 2nd Floor
P.O Box 30091 - 00100, Nairobi – Kenya

Implementers

The Ministry of Interior and National Administration