THE REPUBLIC OF KENYA

NATIONAL CYBERSECURITY STRATEGY

2022

FOREWORD

HE, HON. UHURU KENYATTA, C.G.H.
President of the Republic of Kenya and Commander-in-Chief of the Defence Forces

My fellow Kenyans:

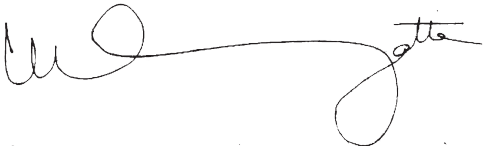
The Republic of Kenya recognizes cyberspace as a new strategic high ground in the envisioned fifth industrial revolution that represent much more advanced collaborative interactions between humans, machines, processes and systems. Driven by increased connectivity and wide adoption of digital technologies, cyberspace has become the new nervous system supporting the functioning and delivery of services to citizens by Kenyan Government and businesses.

As digital technologies continue to offer enormous socio-economic opportunities to our nation and citizens, we are faced with increasing cybersecurity risks and challenges. Cyberspace, with its unlimited borders, has therefore become the most active threat domain providing cyber threats with unparalleled opportunities to harm our nation. Kenya like many countries, is now exposed to dangers posed by foreign and domestic cyber criminals who are state and non-state actors, capable of disrupting provision of essential services, engaging in espionage, and threatening safety and security of our nation.

My Government has identified cybersecurity as a key enabler for digital economy. To protect our digital economy, we are committed to safety and security in all spheres including the cyber domain. Notably, Kenya has adapted various policies, operational and administrative initiatives to improve our national cybersecurity. In strengthening the cybersecurity legislative framework, we enacted the Computer Misuse and Cybercrimes Act 2018 that established the National Computer and Cybercrimes Coordination Committee to coordinate cybersecurity matters. Further, we have enacted the Data Protection Act 2019 to ensure privacy of our data.

I note that a robust National defense and protection of Kenya requires integrity of our physical borders and cyberspace. Therefore, measures to keep our people safe, our critical infrastructure protected and our economy growing are of high priority.

My government has therefore developed this second National Cybersecurity Strategy to renew our efforts of building a secure and resilient cyberspace through a coordinated approach while maximizing on the benefits of a digital economy. As we continue leading in the digital economy in Africa, we aspire to showcase leadership in cybersecurity in the continent. This will be achieved through a coordinated national cybersecurity governance, and investing more in capabilities and capacity. Cybersecurity is a shared responsibility and this Strategy therefore calls all of us to participate in its implementation towards achieving our vision of a safe and trusted cyberspace for people of Kenya.



His Excellency, Hon. Uhuru Kenyatta, C.G.H.
President of the Republic of Kenya
and Commander-in-Chief of the Defence Forces

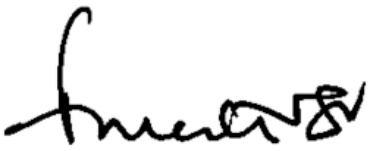
PREAMBLE

DR. FRED OKENGO MATIANG'I, E.G.H.
Cabinet Secretary,
Ministry of Interior and Co-ordination of National Government

Cybersecurity continues to draw considerable attention from Governments across the world. This is because, most services today are dispensed through ICT systems that are in use in all sectors of our economy. The adoption of these technologies has also seen steady growth in cybercrime in the recent times. Notably, the dynamic nature of cyberspace and constantly evolving tactics of perpetrators continue to pose serious risks to peace and stability of our nation.

To respond to this, it has become increasingly necessary for the Government of Kenya to secure her cyberspace. The Government thus, has continued to develop and implement initiatives to combat increasing cybercrimes and strengthen the safety and resilience of our national critical systems. The initiatives include policy formulation and reviews, enactments of laws and regulations, strengthening of governance structures, capacity building, increased awareness programmes and fostering collaboration.

To sustain these cybersecurity efforts, the Government has developed the second National Cybersecurity Strategy setting our priority areas, goals and key interventions. The strategy recognizes the cross-cutting nature of cyberspace and the need for coordinated and collective action from all sectors. In this regard, all stakeholders are encouraged to cooperate and support the Government in creating a more secure environment for our business and day to day activities.



Dr. Fred Okengo Matiang'i, E.G.H.
Cabinet Secretary,
Ministry of Interior and Co-ordination of National Government

MESSAGE

JOE MUCHERU, E.G.H.
Cabinet Secretary,
Ministry of ICT, Innovation and Youth Affairs

The Kenyan government recognizes ICT sector as a key contributor and enabler in attainment of the Vision 2030 to transform Kenya into a digital economy. Guided by key policy documents including the Digital Economy Blueprint, National ICT Policy and National Digital Masterplan, the ICT sector has continued to be a key contributor to the GDP and source of national economic growth. The ICT sector has been instrumental in providing digital tools and innovations necessary to implement the development agenda including the Big Four Agenda as well as building resilience against the effects of economic shocks such as the Covid-19 Pandemic.

To build a robust ICT ecosystem, the Kenyan government in collaboration with businesses is investing in the key pillars for digital economy: Digital Infrastructure; Digital Government services; Digital Business; Digital Skills; Digital Innovations as well as enhancing the policy, legal and regulatory framework. This has seen Kenya register significant progress in adoption of ICT in the delivery of services on digital platforms by government and businesses. The number of e-services for government and businesses has increased making them accessible, convenient and affordable to Kenyan citizens. Similarly, we have enhanced digital connectivity linking the entire government, counties, sub-counties, hospitals, schools and other public service organizations across the Republic of Kenya. Further, we have established more local data centres to ensure strategic data is localized and stored with minimal risk and at low cost. With increased capacity and capability, Kenya has ultimately increased the levels of mobile, Internet penetration and digital innovations in the country.

Despite these notable achievements, Kenya faces increased cybersecurity challenges and risks that threaten the national security and our digital transformation agenda. With increased digital connectedness, Kenya is now more prone to cyber-criminal activities from any part of the world. Our expanded digitalization programmes coupled with investment in digital and data infrastructure present new challenges that require renewed efforts to enhance Kenya's capacity and capability to support the growth of digital economy.

Therefore, the Ministry of ICT, Innovation and Youth Affairs and in collaboration with other stakeholders will continue to prioritize formulation and review of policies, laws and regulations and implementation of key initiatives aimed at building a safe and secure cyberspace as envisioned by this National Cybersecurity Strategy.

Joe Mucheru, E.G.H.
Cabinet Secretary,
Ministry of ICT, Innovation and Youth Affairs

CONTENTS

LIST OF ACRONYMS

AG	– Attorney General
CA	– Communications Authority
CBK	– Central Bank of Kenya
CII	– Critical Information Infrastructure
CIRT	– Computer Incident Response Team
CMCA	– Computer Misuse and Cybercrimes Act
DCI	– Directorate of Criminal Investigations
DPA	– Data Protection Act
GoK	– Government of Kenya
ICT	– Information, Communications and Technology
ISMS	– Information Security Management System
KE-CIRT	– Kenya Cyber Incident Response Team
KDF	– Kenya Defense Forces
KICA	– Kenya Information and Communications Act
KICD	– Kenya Institute of Curriculum Development
KIPPRA	– Kenya Institute for Public Policy, Research and Analysis
MCDAs	– Ministries, Counties, Departments and Agencies
MIIYA	– Ministry of ICT, Innovation and Youth Affairs
MoI	– Ministry of interior and coordination of national government
MoD	– Ministry of Defence
MoE	– Ministry of Education
NC4	– National Computer Cybercrimes and Coordination Committee
NIS	– National Intelligence Service
NPS	– National Police Service
NSOC	– National Cybersecurity Operation Center
NTSA	– National Transport and Safety Authority
ODPP	- Office of the Director of Public Prosecutions
PSC	– Public Service Commission
SOC	– Cybersecurity Operation Centre

LIST OF FIGURES

EXECUTIVE SUMMARY

The National Cybersecurity Strategy 2022 provides direction for a unified approach in the implementation of cybersecurity activities in Kenya. The Strategy establishes foundations and pillars for effective cybersecurity for public and private sector by combining good governance with a set of initiatives and interventions. The Strategy commences with an in-depth background of Kenya's cybersecurity landscape that highlights existing policy, legal and regulatory frameworks as well as outlining the challenges and threats facing Kenya's cyberspace.

The Strategy's vision is a safe and trusted cyberspace for the people of Kenya; and a mission to build a secure and resilient cyberspace through a coordinated approach while maximizing on the benefits of a digital economy. The Strategy further provides a framework to defend and protect the cyberspace of the Republic of Kenya guided by the following strategic pillars:

1. Cybersecurity governance;
2. Cybersecurity policies, laws, regulations and standards;
3. Critical Information Infrastructures Protection (CIIP);
4. Cybersecurity capability and capacity building;
5. Cyber-Risks & Cyber-Crimes Management; and
6. Co-operation and collaboration

The Strategy also has an implementation matrix which outlines the strategic interventions related to the Strategic Pillars. The matrix assigns roles and responsibilities to various cybersecurity actors to be performed within specified timelines as well as estimated costing of the initiatives.

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.

CHAPTER 1: INTRODUCTION

1.1 Background

Cyberspace is fundamental to the functioning of national and international security systems, trade networks, emergency services, basic communications, and other public and private activities. Cyberspace comprises of the network that connects various Information, Communication and Technology (ICT) infrastructure and includes: Internet, telecommunication networks, the Internet of Things (IoT), various computer systems, mobile communications, and interactions between virtual space and people constituted by information and data. Cyberspace has become a second space for human production and life and stands in juxtaposition to the real spaces of land, sea, air and outer space as the fifth largest strategic space.

However, the wide adoption and the evolving nature of cyberspace primarily driven by emerging technologies has created new risks. These risks expose individuals, businesses, national infrastructure and government to cyber threats emanating from a wide variety of sources (state and non-state) and which manifest themselves in disruptive activities. Their effects carry significant risk to public safety, security of the nation and stability of the globally linked economy.

The Government of Kenya (GoK) continues to initiate and promote numerous cybersecurity policy and legal initiatives. For instance, the Government developed and enacted various policy, legal and regulatory frameworks aimed at leveraging the opportunities of digital transformation to improve Kenya's economic development while ensuring digital safety of its people, businesses and interests. Key ICT policies, legal and regulatory frameworks include: Kenya Information and Communications Act, 1998; National Cybersecurity Strategy 2014; National Broadband Strategy 2018; Computer Misuse and Cybercrimes Act (CMCA), 2018; Data Protection Act (DPA), 2019; National ICT Policy Guidelines 2020; and National Digital Master Plan 2022.

Kenya developed her first Cybersecurity Strategy in 2014, with the vision, key objectives, and commitment to support national priorities by encouraging ICT growth and proactive protection of critical information infrastructures. Through the 2014 Strategy; Kenya established Kenya Computer Incident Response Team and coordination Centre (KE-CIRT/CC) and the National Digital Forensics Laboratory at the National Police Service under

Directorate of Criminal Investigations (DCI). In regard to legislation, the Government enacted the Computer Misuse and Cybercrimes Act-2018 which is currently the overarching law for protection of Critical Information Infrastructures and management of cybercrime in Kenya. To achieve its objectives, the Act establishes and mandates the National Computer and Cybercrimes Co-ordination Committee (NC4) and the Secretariat, as the national authority to spearhead and coordinate cybersecurity matters. The Committee comprises of Principal Secretary in charge of internal security, Principal Secretary in charge of ICT, Attorney-General (AG), Chief of the Kenya Defence Forces (CDF), Inspector-General of NPS, Director-General NIS, Director-General CA, Director of Public Prosecutions (DPP), Governor CBK, and Director NC4 Secretariat.

To initialize CII protection as provided by the CMCA, GoK designated sectors and critical systems that facilitate provision of essential services and are strategic to national security as Critical Information Infrastructures (CIIs) vide the Gazette Notice No.1043 of 31 January 2022. These are systems whose disruption would result in: interruption of life sustaining service; an adverse effect on the economy of the Republic of Kenya; an event that would result in massive casualties or fatalities; failure or disruption of money market of the Republic of Kenya; and adverse and severe effect on the security of the Republic of Kenya including Intelligence and Military services. This affirms the Republic of Kenya's commitment to safeguard and protect Kenya's sovereignty and its people.

1.2 Cybersecurity Strategy Rationale

The Republic of Kenya identifies cybersecurity as a national economic and security challenge. The most prevalent cybersecurity challenges in Kenya include exploitation of the new operating environment by adversaries to conduct war like activities such as disruption of operations of critical infrastructure. Most ICT infrastructure and users in the Republic of Kenya have prioritized efficiency, cost and convenience and overlooked security during development and implementation. Interconnected ICTs have inherent vendor/manufacturer vulnerabilities that can be exploited by adversaries and expose Kenyan citizens, businesses and government to global threats. Despite a growing number of incidents, governance of cyberspace has remained uncoordinated with no clear structure. While Kenya has enacted various policies and laws, regular review and update is necessary in order to effectively address emerging risks and

threats. Further, cybersecurity awareness of government employees and the general public is assessed to be low thus increasing susceptibility to cybersecurity threats.

On the other hand, Kenya increasingly continues to face cybersecurity threats (see figure 1) leveraging on the above-mentioned challenges. Nation states and corporate entities have used cyber espionage to gain access to sensitive/classified data for financial gain, political reasons and to gain competitive advantage. Further, as ICTs become more interconnected, systems become susceptible to sabotage through deliberate and malicious acts that may disrupt normal processes and functions or destroy/damage equipment and information. Similarly, Cyber subversion through propaganda, fake news and misinformation may undermine trust in the government, authority and competence of leaders thus posing a threat to Kenya's stability. In addition, terror groups continue to leverage on ICTs (virtual private networks, internet, global applications, social media platforms and websites) for recruitment, radicalization, incitement, financing, training, planning and execution of attacks. Also, there has been an increase in cyber fraud cases through banking/finance, sim swaps and online scams such as digital Ponzi schemes, job scams, fake websites & lotteries, Crypto and Forex Scams, "Tuma kwa Hii Namba" syndicates among others

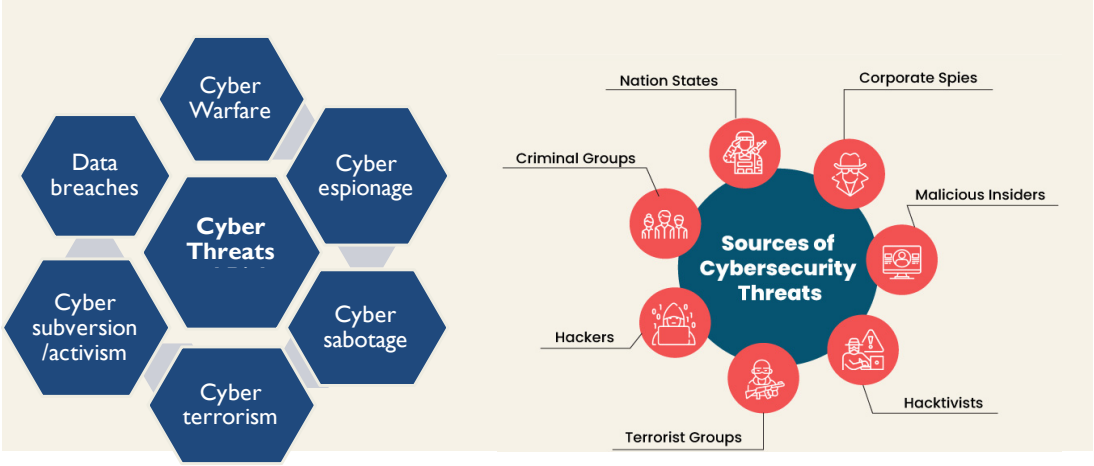


Figure 1: Threats and Actors

Cybersecurity statistics indicate that the number of cyber threats detected in Kenya has significantly increased in the last three years. For instance, 143,040,599 cyber threats were detected in July-September 2021 as compared to 4589 threats detected in July-September 2017 (see figure 2).

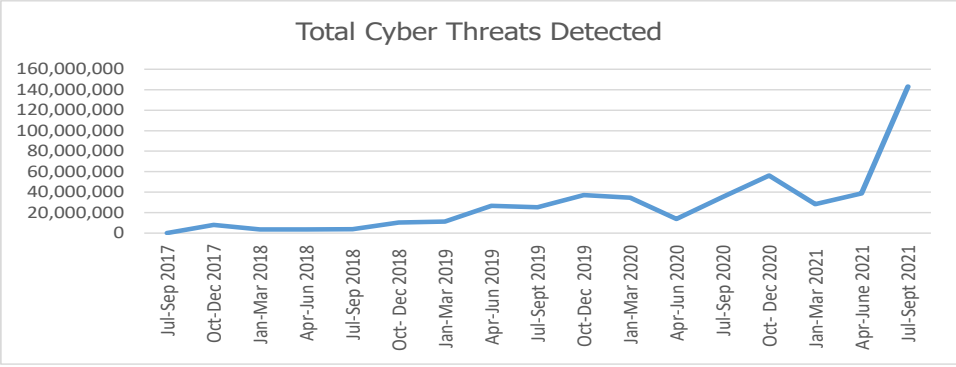


Figure 2: Total Cyber Threats Detected
Source: KIPPRA 2022 (Computed from various CA reports)

To facilitate actualization of GoK cybersecurity initiatives, and address the above challenges and threats, this Strategy aims to enhance institutional framework for cybersecurity governance and coordination; strengthen cybersecurity policy, legal and regulatory frameworks; enhance the protection and resilience of CIIs; strengthen cybersecurity capability and capacity; minimize cybersecurity risks and crimes and foster national and international cooperation and collaboration.

GoK will spearhead its main responsibility of defending the Republic of Kenya's cyberspace from all threats, to protect Kenyan citizens and the economy from harm, and to establish domestic and international frameworks to safeguard national interests, protect fundamental rights, and prosecute offenders.

Similarly, Critical Information Infrastructure owners/operators, businesses and organizations in Kenya have the obligation of implementing measures to protect their critical systems and services by adopting a risk-based approach towards cybersecurity, managing vendor cybersecurity risks, adopting minimum cybersecurity baseline standards and supporting the government through reporting and response to cybersecurity matters.

Finally, Kenyan citizens and non-citizens must take precautions to protect themselves and their valued possessions in the virtual world, just as they do in the physical world. That involves taking all reasonable precautions to protect not only the hardware – phones, computers and other gadgets, but also the data, software, and systems that provide freedom, flexibility, and convenience in their personal and professional lives.

1.3 Strategy Development and Implementation Process

Kenya Cybersecurity Strategy 2022 development and implementation process entailed five phases; initiation, stocking and analysis, production, implementation and Monitoring & Evaluation (see figure 3) in line with Kenya's public policy formulation approach and international best practices. NC4 initiated the Strategy formulation by establishing the National Cybersecurity Strategy Steering Committee who developed a work plan with major steps and activities, key stakeholders, timelines, human, and financial resource requirements. During stocking and analysis, the national cybersecurity capacity status was used to collect data on the strategic national cybersecurity posture and risk landscape that informed drafting of the Strategy. The production phase entailed several meetings and multi-stakeholder workshops that generated this Strategy. The implementation phase entails involving multi-stakeholders to support the execution of the identified initiatives in this strategy. While Monitoring and Evaluation phase is based on the National Integrated Monitoring and Evaluation System (NIMES) framework.

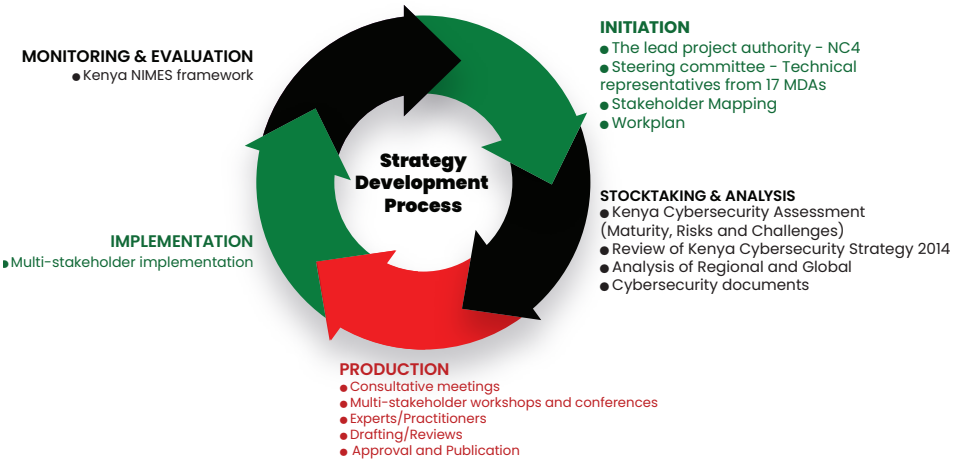


Figure 3: Strategy Development and Implementation Process

CHAPTER 2: STRATEGIC FOUNDATIONS

2.1 Guiding Principles

The guiding Principles of the Kenya Cybersecurity Strategy 2022 are based on the following objectives of the Computer Misuse and Cybercrimes Act, 2018:

1. Protect the confidentiality, integrity and availability of computer systems, programmes and data;
2. Prevent the unlawful use of computer systems;
3. Facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes;
4. Protect the rights to privacy, freedom of expression and access to information as guaranteed under the constitution of Kenya 2010; and
5. Facilitate international cooperation on cybersecurity matters.

In addition, the Strategy is guided by Kenya's public policy formulation process and international best practices.

2.2 Vision

Safe and trusted cyberspace for the people of Kenya.

2.3 Mission

To build a secure and resilient cyberspace through a coordinated approach while maximizing on the benefits of a digital economy.

2.4 Strategy Goals

The following are the goals of the Strategy:

1. Enhance Kenya's institutional framework for cybersecurity governance and coordination.
2. Strengthen cybersecurity policy, legal and regulatory frameworks.
3. Enhance the protection and resilience of CIIs.
4. Strengthen cybersecurity capability and capacity.
5. Minimize cybersecurity risks and crimes.
6. Foster national and international cooperation and collaboration.

2.5 Strategy Pillars

The Strategy is based on the following pillars:

1. Cybersecurity governance;
2. Cybersecurity policies, laws, regulations and standards;
3. Critical Information Infrastructures Protection (CIIP);
4. Cybersecurity capability and capacity building;
5. Cyber-Risks & Cybercrimes Management; and
6. Cooperation and collaboration.

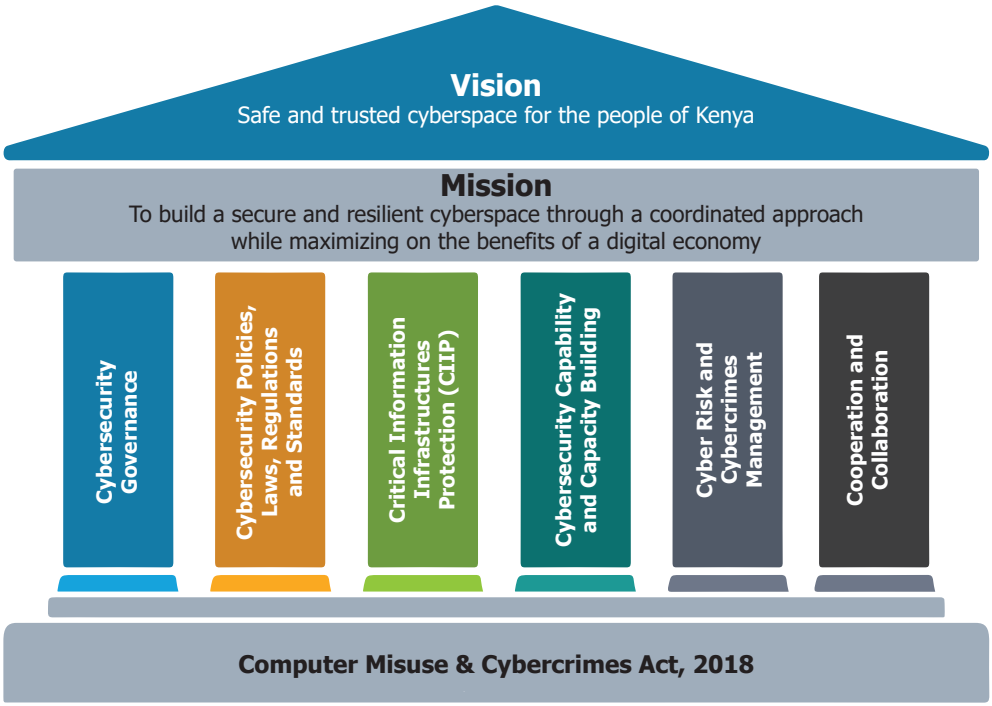


Figure 4: Kenya Cybersecurity Strategy Foundations

CHAPTER 3: STRATEGIES

3.1 Cybersecurity Governance

Cybersecurity governance is critical in developing a vibrant cybersecurity ecosystem for a digital economy. Figure 5 provides the cybersecurity governance structure linking all the key actors through NC4 to the National Security Council. Enhancing Kenya's cybersecurity governance will lay foundations for protecting Kenya from cyber threats in the long term.

The Cybersecurity governance pillar provides strategic guidance on governance structures and resources required to support formulation and implementation of a secure national cyber ecosystem. The goal, objective and interventions in this pillar are:

***Goal*:**

Enhance Kenya's institutional framework for cybersecurity governance and coordination.

***Objective*:**

Improve governance, resource allocation and coordination of cybersecurity in Kenya.

***Interventions*:**

a. Allocate the NC4 Secretariat with dedicated budget, human capacity, infrastructure and tools to effectively support NC4 implement its mandate.

b. Review the multi-agency governance structure by establishing an autonomous cybersecurity entity (National Cybersecurity Agency).

c. Upgrade the Kenya Computer Incident Response Team (KE-CIRT) to the National Multi-Stakeholder Computer Incident Response Team of the Republic of Kenya.

d. Establish a National Cybersecurity Operation Centre (NSOC).

e. Establish/Enhance Cybersecurity Operation Centers (SOC) in CIIs.

f. Establish/enhance specialized cybersecurity units and Sector CIRTs (Defence, Intelligence, Police, Public Prosecutions, Judiciary and Sector CIRTs).

g. Establish Joint Cybersecurity technical working groups.

Outcome:

Effective governance and coordination of cybersecurity in Kenya.

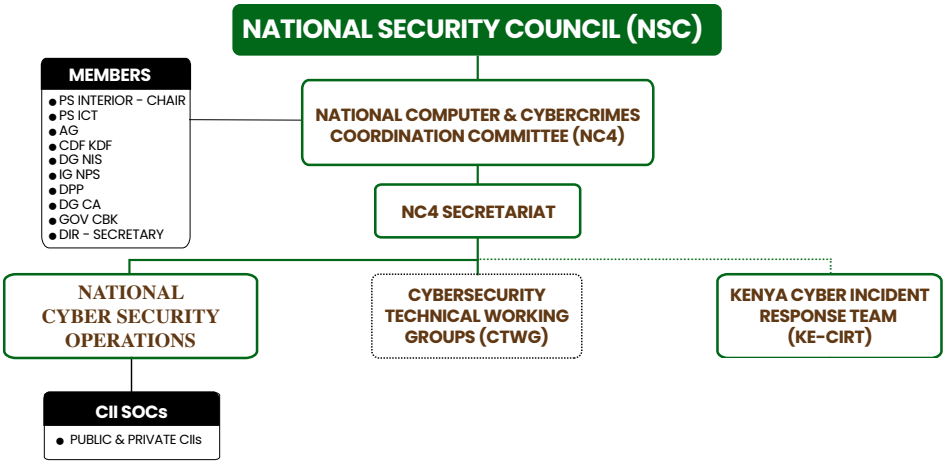


Figure 5: Cybersecurity Governance Structure

3.2. Cybersecurity Policies, Laws, Regulations & Standards

Development of a safe, secure and resilient cyberspace ecosystem requires a robust policy, legal and regulatory framework. Figure 6 outlines all the key components and their relationship in the design and implementation of an Information Security Management System (ISMS) which is a key target in securing information assets in Kenya.

Enhancing Kenya's effort to formulate and implement coherent cybersecurity policy, legislation, regulations and standards will require the involvement of key actors drawn from both the public and private sector. The goal, objective and interventions in this pillar are:

Goal:

Strengthen cybersecurity policies, laws, regulations and Standards.

Objective:

Have up-to-date cybersecurity policies, laws, regulations and standards.

Interventions:

a. Review cybersecurity policies, laws, regulations and standards.
b. Amend/update cybersecurity policies, laws, regulations and standards.

c. Establish new cybersecurity policies, laws and regulations for: implementation of CMCA-2018; adoption of new and emerging technologies; outsourcing of critical systems; adoption of country code top level domain ".ke" among others.

d. Establish national cybersecurity standards/architecture.

Outcome:

Coherent and effective cybersecurity policies, laws, regulations and standards.

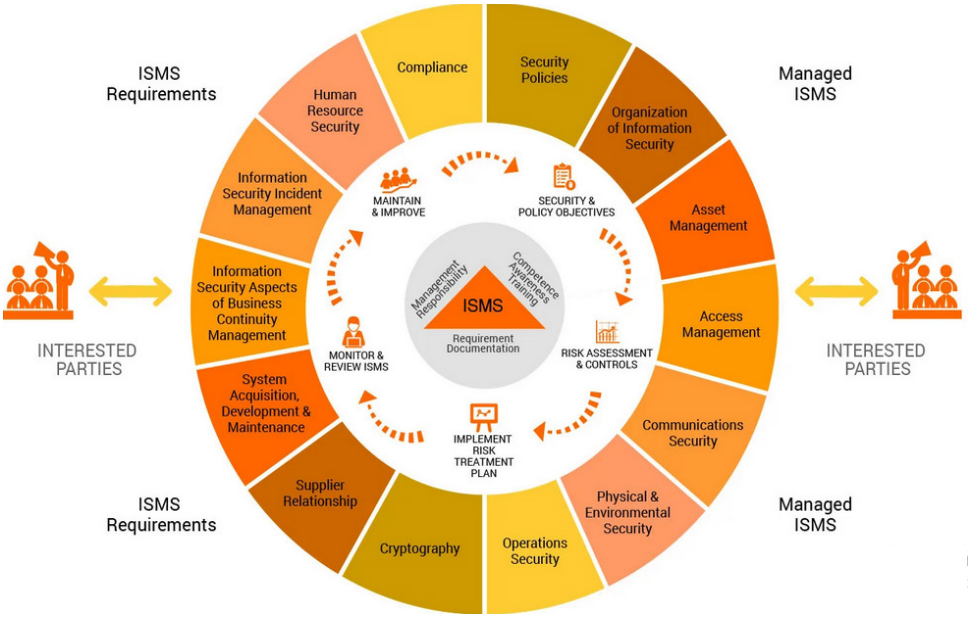


Figure 6: Information Security Management System

Source: ISMS Alliance

3.3 Critical Information Infrastructure Protection (CIIP)

With increasing digitalization, CIIs that were previously isolated from the internet across many sectors (see figure 7) are now increasingly linked to other digital systems, exposing them to cyber threats, and thus compromising national security and public safety. The Kenyan government is committed to implement various initiatives in an effort to improve the cybersecurity posture and resilience of CIIs and other digital systems and infrastructure. The goal, objective and interventions in this pillar are:

Goal:

Enhance the protection and resilience of CIIs.

Objective:

Protect and safeguard CIIs.

Interventions:

a. Develop Critical Information Infrastructure Protection framework.
b. Identify and classify CIIs.
c. Implementation of Cryptography and access control to safeguard GoK sensitive information and data.
d. Implement baseline cybersecurity measures (physical and technical security controls including emergency/disaster contingency and recovery measures).
e. Encourage establishment of in-country Cloud Computing Data Centers and services, and promote local hosting.
f. Promote use of local internet exchange points.
g. Establish Information sharing/reporting and Incident response framework.

Outcome:

Increased protection and resilience of CIIs.

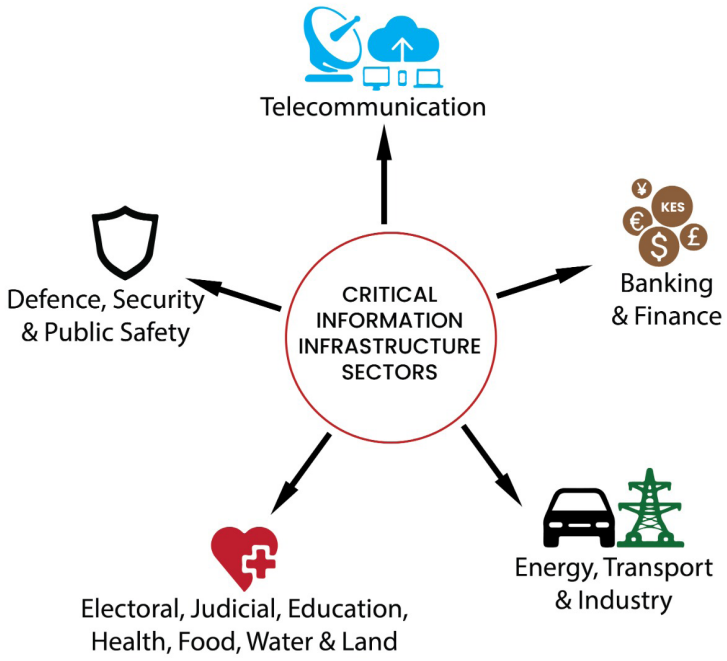


Figure 7: Critical Information Infrastructure sectors, Gazette Notice No. 1043 of 31st January, 2022

3.4 Capability & Capacity Building

Threats and risks in the cyberspace are becoming more sophisticated as technology develops. To ensure the availability of cutting-edge capabilities amidst rapid technology change, the Kenyan Government will support advanced research, foster local digital innovation, and develop local cybersecurity skills and knowledge to position Kenya as a continent leader in cybersecurity.

The demand for qualified cybersecurity professionals represents an immediate and growing opportunity in the cybersecurity sector. The Government will therefore work together with academia, research institutions and private sector to create new opportunities, drive investment, and foster leading-edge research and development in cybersecurity. The goal, objective and interventions in this pillar are:

Goal:

Strengthen cybersecurity capability and capacity.

3.4.1 Cybersecurity Capability

Objective:

Enhance cybersecurity protection and resilience.

Interventions:

a. Establish a national cyber Defence/Protection framework.
b. Develop a cyber-defense Strategy for the Republic of Kenya.
c. Implement the necessary cybersecurity protection, detection, analysis, and response tools/system to defend Kenya's digital environment.
d. Develop a Cybersecurity Innovation, Research and Development (R&D) framework.
e. Promote cybersecurity R&D of in-country secure, competitive, cost-effective and tailor-made cybersecurity solutions.

Outcome:

Increased cyber protection against, and response to cybersecurity threats/incidents.

3.4.2 Cybersecurity Capacity

Objective:

Increase cybersecurity expertise, education and awareness.

Interventions:

a. Establish a cybersecurity professional certification/accreditation and career progression framework.

b. Establish a Cybersecurity Centre of Excellence (CCoE).

c. Develop more local specialized experts in cybersecurity.

d. Develop and implement cybersecurity basic education curriculum.

e. Develop and implement cybersecurity awareness raising programme.

Outcome:

Increased cybersecurity capacity and improved cybersecurity culture.

3.5 Cyber-Risks & Cyber-Crimes Management

With increased number of cyber risks as well as malicious and complex threats, there is need to put measures for quick detection and remediation of such threats. To strengthen capabilities to protect, detect, respond, and recover from malicious cyber activities, Kenya will enhance its cyber risks and cybercrime management.

The Government is committed to protect Kenyans from cybercrime, respond to evolving threats, defend critical systems and ensure cyber-physical risks are well managed. The goal, objective and interventions in this pillar are:

Goal:

Minimize cybersecurity risks and crimes.

Objective:

Mitigate cybersecurity risks and combat cybercrimes.

***Interventions*:**

a. Develop and implement a national cybersecurity risks management framework.
b. Perform national cybersecurity risk assessment/audits.
c. Develop and implement a national framework for cybercrime management.
d. Establish a National Cybercrimes Alert and Warning system.

***Outcome*:**

Reduced cybersecurity risks and crimes.

3.6 Co-operation & Collaboration

Cyber threats are cross-cutting and transnational. This require co-operation and collaboration at national and international levels. Strengthening engagement and collaboration with all stakeholders to develop mechanisms and policies, and implement cybersecurity initiatives will contribute to a secure and resilient cyberspace at national and international levels. The Kenyan Government is committed to work with internal stakeholders such as academia, research institutions and private sector as well as international partners to improve Kenya's cybersecurity posture. The goal, objective and interventions in this pillar are:

***Goal*:**

Foster national and international co-operation and collaboration.

***Objective*:**

Improve national and international co-operation and collaboration.

***Interventions*:**

a. Develop a national framework for national, regional and international co-operation and collaboration.
b. Establish a trusted information sharing mechanism for information exchange and incident reporting for national and international stakeholders.
c. Participate and promote the development and implementation of international laws, agreements, treaties, policies, norms, standards, conferences and fora on cybersecurity.

Outcome:

Well-coordinated co-operation and collaboration that strengthens Kenya's cybersecurity.

CHAPTER 4: IMPLEMENTATION FRAMEWORK

4.1 Strategy Implementation

Implementation of the Kenya Cybersecurity Strategy 2022 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.

4.1.1 Implementation Matrix

S/No	STRATEGY PILLAR	INTERVENTION	ACTIVITIES	TIMELINES		KEY ENTITIES
				START	END	
(a)	(b)	(c)	(d)	(e)		(f)
1.	Cybersecurity Governance	Resources & dedicated cybersecurity budget	NC4 & NC4 Secretariat dedicated budget, (Human capacity, infrastructure and tools).	July 2022	June 2027	Ministry of Interior National Treasury MIIYA PSC AG NC4 & Secretariat International Partners
			Establish the NC4 Secretariat as an autonomous entity (National Cyber Security Agency- NCSA).	June 2023	July 2026	
			Establish a National Cyber Security Operation Centre (NSOC).	July 2022	June 2024	NC4 & Secretariat Ministry of Interior MoD MIIYA
			Upgrade the Kenya Computer Incident Response Team (KE-CIRT) to the National Multi-Stakeholder Computer Incident Response Team of the Republic of Kenya.	July 2022	June 2024	
			Support the establishment/ enhancement of Cybersecurity Operations Centers (CSOCs) in CIIs.	July 2022	June 2027	NC4 & Secretariat Ministry of Interior Office of AG CII Sectors CIIs Operators/Owners
			Support specialized cybersecurity units (KDF, NIS,NPS, ODPP, Judiciary) and Sector CIRTs	July 2022	June 2027	NC4 & Secretariat Ministry of Interior MoD ODPP Judiciary Sector Regulators
			Cybersecurity technical working groups.	July 2022	June 2027	NC4 & Secretariat Academia MCDAs CBK CIIs Operators/Owners International Partners

S/No	STRATEGY PILLAR	INTERVENTION	ACTIVITIES	TIMELINES		KEY ENTITIES
				START	END	
(a)	(b)	(c)	(d)	(e)		(f)
2.	Cybersecurity Policies, Laws, Regulations & Standards	Develop cybersecurity regulations.	Develop CMCA-2018 Regulations	July 2022	June 2024	NC4 & Secretariat Ministry of Interior MIIYA MFA AG Judiciary KIPPRA KLRC CIIs KEBS Parliament
			Develop regulations for outsourcing of critical systems, adoption of new technologies and application of country code top level domain ".ke" in Kenya.	July 2022	June 2025	
		Review/ Amend the Kenya ybersecurity legal and regulatory framework	Review and amend the CMCA-2018 and other laws on secure use of ICTs.	July 2022	June 2027	
			Update cybersecurity regulations and standards.	July 2022	June 2027	
		Establish national cybersecurity standards/ architecture	Develop Kenya Cybersecurity architecture.	July 2022	June 2023	
			Review and enhance implementation Kenya's cybersecurity architecture.	July 2022	June 2027	
			Accredit and certify ICT products, new technologies, services and suppliers on compliance to the National cybersecurity standard.	July 2022	June 2027	

S/No	STRATEGY PILLAR	INTERVENTION	ACTIVITIES	TIMELINES		KEY ENTITIES
				START	END	
(a)	(b)	(c)	(d)	(e)		(f)
3.	Critical Information Infrastructure Protection (CIIP)	Develop and implement a CIIP framework.	Identify and classify CIIs.	July 2022	June 2027	NC4 & Secretariat Ministry of Interior MoD MIIYA CIIs Operators/Owners Sector Regulators
			Implementation of Cryptography and access control to safeguard GoK sensitive information and data.	July 2022	June 2027	
			Promote use of local internet exchange points.	July 2022	June 2027	
			Encourage establishment of in-country Cloud Computing Data Centers and services, and promote local hosting.	July 2022	June 2027	
			Establish Information sharing/reporting and Incident response framework.	July 2022	June 2027	
			Implement baseline cybersecurity measures (physical and technical security controls including emergency/disaster contingency and recovery measures).	July 2022	June 2027	

(a)	(b)	(c)	(d)	(e)		(f)
4.	Capability & Capacity Building	Establish a national cyber Defence/ Protection and resilience framework.	Develop a cyber-Defence strategy.	July 2022	June 2024	NC4 & Secretariat MoD Ministry of Interior MIIYA MFA CIIs Operators Sectoral CIRTs
			Develop a national cyber Defence/ Protection and resilience framework, and implement the National Cybersecurity Intrusion, Prevention, Detection and Mitigation (NCIPDM) system.	July 2022	June 2024	
		Develop a Cybersecurity Innovation, Research and development framework	Promote cybersecurity R&D of in-country secure, competitive, cost-effective and tailor-made cybersecurity solutions.	July 2022	June 2027	NC4 & Secretariat MoE MoD Ministry of Interior MIIYA MoT&I KIPPRA Academia International Partners CII Operators/ Owners MoPSSP Global Tech Companies Media Others
		Establish a cybersecurity professional certification/ accreditation and career progression framework.	Establish a Cybersecurity Centre of Excellence (CCoE).	July 2022	June 2027	
			Develop local specialized experts in cybersecurity.	July 2022	June 2027	
			Develop/implement cybersecurity basic education curriculum.	July 2022	June 2027	
		Develop/ implement cybersecurity awareness raising curriculum.	Establish a national Cybersecurity awareness curriculum	July 2022	June 2027	
			Establish platforms and channels for cybersecurity awareness.	July 2022	June 2023	
			Implement cybersecurity awareness programmes.	July 2022	June 2027	
			Promote programmes and exercises for awareness-raising.	July 2022	June 2027	
			Observe the cybersecurity awareness month in Kenya.	July 2022	June 2027	

5.	Cyber-Risks & Cyber-Crimes Management	Develop and implement a national cybersecurity risks management framework.	National cybersecurity risk assessment/audits.	July 2022	June 2027	Ministry of Interior MoD MIIYA CBK CA KRA NC4 & Secretariat Office of the Auditor General MCDAs CII Operators/ Owners International Partners
		Develop and implement a national framework for cybercrime management.	Establish a National Cybercrimes Alert and Warning system.	July 2022	June 2024	
6.	Cooperation & Collaboration	Develop a national framework for national, regional and international cooperation and collaboration.	Establish a trusted information sharing platform for information exchange and incident reporting for national and international stakeholders.	July 2022	June 2024	NC4 & Secretariat Ministry of Interior MoD MIIYA MFA Office of AG ODPP International Partners
			Participate and promote the development and implementation of international laws, agreements, treaties, policies, norms, standards, conferences and fora on cybersecurity.	July 2022	June 2027	

4.2 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.

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