Republic of Zambia

Ministry of Transport
and Communications

National Cybersecurity Policy

March 2021

Contributors

This policy was developed by the Ministry of Transport and Communication (MTC) and the Zambia Information and Communications Technology Authority (ZICTA), including other stakeholders.

Authors, editorial, production, research,

Mr. Yese Bwalya (MTC)
Mr. Stephen Mbewe (MTC)
Mr. Khumbuzo Nkunika (MTC)
Mr. Austin Sichinga (MTC)
Ms. Sylvia Mulenga (MTC)
Ms. Irene Tembo (MTC)
Mr. Victor Kulukulu (MTC)
Ms. Clara E. Phiri (MTC)
Mr. Sydney Tembo (MTC)
Mr. Patrick Mutimushi (ZICTA)
Mr. Thomas Malama (ZICTA)
Mr. Mwenya Mutale (ZICTA)
Mr. Nawa T.J. Samatebele (ZICTA)
Ms. Banji Nyundo (ZICTA)
Ms. Ngabo Nankonde (ZICTA)
Ms. Chewe Mutale (ZICTA)
Ms. Chipo Mwiinde (ZICTA)

Design & Layout

Mr. Paul Sinyinda (ZICTA)

National Cybersecuirty Policy 2021

Foreword

The Zambian Government and private sectors continued rollout and investment in Information and Communications Technology (ICT) networks and systems has increased access to ICTs and the internet. These have been powerful tools for human and economic development which have simplified provision of health care, financial services, education, agriculture, mining, commerce, transportation, banking, manufacturing, energy, trade, media and broadcasting services, amongst others.

Zambia's cyberspace has also experienced continuous development. With a substantial increase in access to the internet in the country, concerns around cybersecurity have become prominent. Access to the internet has brought about a new type of risk and threat to national peace which in itself will need new forms of defence to counter it. The country remains at risk of eminent cybersecurity incidents that may significantly disrupt the healthy functioning of our cyber eco-system emanating from both local and/or international threats. Cyber-attacks are growing in prominence every day and the role these attacks play in our daily lives should not be underestimated. The average cost of combating malicious software and data breaches continues to increase, making the recovery from cybercrimes very costly to businesses. .

The aim of this Policy is to establish a coordinated cybersecurity framework and enhance resilience of national ICT systems to cyber incidents in order to attain the desired transformation into a Smart Zambia that is underpinned by trust and confidentiality. The Policy also aims at reforming the legal and regulatory framework on cybersecurity and cybercrimes in the country.

Successful implementation of this Policy will require extensive collaboration with all stakeholders. As the Ministry responsible for the development of the ICTs, we will endeavour to put in place a multi-sectoral framework that allows all stakeholders to play their role in the prevention and detection of and recovery from cyber-attacks and incidences. Due to the borderless nature of cybersecurity, Zambia will work closely with other countries within the SADC Region, African Union, United Nations and indeed other organisations in order to foster international cooperation in fighting against the increasing number of incidents caused by illegal activities in cyberspace.

Hon. Mutotwe L. Kafwaya, MP
Minister of Transport and Communications

Acknowledgement

The primary responsibility of the Government is to preserve the country's peace and tranquillity and ensure that all forms of attack on sovereignty are thwarted both through stronger defences and better cyber skills.

The Ministry of Transport and Communications (MTC) commits to enhancing the resilience of Zambia's national ICT systems and ensuring a safer Zambian cyber space as this will contribute to the vision set out by the Government to transform the country into a Smart Zambia.

This Policy was developed through extensive consultation. I would, therefore, like to sincerely thank all those who provided valuable diverse input and comments during the process of formulating the Policy. I acknowledge the guidance and support provided by Policy Analysis and Coordination Division, Cabinet Office and the various Ministries.

I would like to also pay tribute to the guidance and support rendered by the members of the National Cyber Security Technical Committee (NCSTC) who provided the groundwork and technical expertise during the entire process of Policy formulation.

Lastly, I would like to thank my team under the MTC specifically, the Department of Communication, Planning and Monitoring Department and Zambia Information and Communications Technology Authority for working tirelessly to ensure that the National Cybersecurity Policy was formulated.

Eng. Misheck Lungu
Permanent Secretary
Ministry of Transport and Communications

Table of Contents

Definitions

In the context of this Policy:

Computer Incident Response Team (CIRT)	means a team of dedicated information security specialists that prepares for and responds to cybersecurity incidents;
Critical Information Infrastructure	means all ICT systems, data systems, databases, networks (including people, buildings, facilities, and processes), that are fundamental to the effective operation of Zambia;
Cyber	means the use, simulated environment or state of connection or association with electronic communications or networks including the internet;
Cybercrime	” means illegal acts, the commission of which involves the use of information and communication technologies;
Cybersecurity	means the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user assets;
Cyberspace	means physical and non-physical terrain created by and/or composed of some of all the following: computers, computer systems, networks, and their computer programmes, computer data, content data, traffic data, and users;
Cyber resilience	means the ability to prepare for, respond to and recover from cyber-attacks;
Cyber warfare	” means actions by a nation/state to penetrate another nation’s computer and networks for purposes of causing damage or disruption;
Digital Financial Service (DFS)	means financial services accessed and delivered through digital channels i.e. internet, mobile, ATMs, POS terminals etc and include payments, credit, savings, remittances and insurance;
Electronic commerce (e-commerce)	also known as internet commerce means the buying and selling of goods and services using the internet, and the transfer of money and data to execute these transactions;
Electronic Communication	means a transfer of signs, signals, writings, images, sounds, data or intelligence of any nature transmitted in whole or in part by radio, electromagnetic, photo-electronic or photo-optical system but does not include- a. Any wire or direct oral communication; b. Any communication made through a tone – only paging device; c. Any communication from a tracking device; or d. Electronic funds transfer information stored by a financial institution in a communication system used for electronic storage and transfer of funds.
Electronic Services (e-services)	means the provision of service using electronic means or via the Internet;
Information and Communication Technology	mean the application of modern communication and computing technologies to the creation, management and use of information through utilising of hardware, software, networks and media for the collection, storage, processing, transmission and presentation of information and related services;
Information society	means people-centred, inclusive and development-oriented information, where everyone can create, access, utilise and share information and knowledge, enabling individuals, communities and people to achieve their full potential in promoting their sustainable development and improving the quality of their life; and
Malware	means malicious software, and its programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviour.

Acronyms

AU	African Union
CII	Critical Information Infrastructure
ECT Act	Electronic Communication and Transactions Act No. 21 of 2009
ICT	Information and Communication Technologies
MTC	Ministry of Transport and Communications
ZmCIRT	Zambia Computer Incident Response Team
ZICTA	Zambia Information and Communications Technology Authority

Chapter 1 — Introduction

Rapid developments in technology, particularly in telecommunications, have created a new world of interconnected communication networks that have transformed society, creating new opportunities and challenges for individuals and society at large.

Cyberspace is a new frontier for a variety of innovations for social and economic progress. The management of Cyberspace is important not only because of the actions of individual participants but also the infrastructure of cyberspace is now fundamental to the functioning of national and international security systems, trade networks, emergency services, basic communications, and other public and private activities. As the world enters its fourth industrial revolution shaped by the immense transformational power of digital technology, it is argued that the countries that will stand to benefit are those that will harness the new technology while safeguarding individual and national interest against a new kind of threat presented by cybercrime.

Although Zambia's journey towards the digital information age dates back many years, the launch of the ICT Policy in 2006 formally recognised ICTs to be critical in achieving national development. The 2006 ICT Policy achieved much in terms of commitments and objectives set forth. However, widespread adoption of ICTs over the years has overtaken the gains of the 2006 ICT Policy. This has been compounded by cyber threats while extensive innovations have unleashed a new wave of cybercrimes. Additionally, other intervening policy measures intended to further leverage and accelerate the nation's move towards an information society and attain middle income status such as Vision 2030, the Seventh National Development Plan and Smart Zambia initiatives have all added a new layer of complexity to the country's cybercrime landscape.

While the country has inadequate national statistics on the nature and incidences of cybercrimes, the menace and prevalence cannot be disputed. Cybercrime in the country, as exemplified by several incidences of electronic fraud and other cyber related criminality in recent past, has been on the rise. This and the need to have a coordinated framework to respond to cyber incidences has necessitated the need for the formulation of the country's first National Cybersecurity Policy. The thrust of this Policy is to ensure a clear, bold and decisive cybersecurity governance structure is developed to direct and drive coordinated efforts to foster defence of the Zambian cyberspace.

The Policy is divided into six parts namely: Introduction, Situation Analysis, Vision, Rationale and Guiding Principles, Objectives and Implementation Framework. The Situation Analysis gives an overview of the cybersecurity situation in the country. The Rationale explains the justification for the Policy and the guiding principles upon which it is grounded. The Policy further outlines the objectives and policy measures and ends with an implementation framework which outlines the institutional arrangements and legal framework to support the implementation of the Policy.

Chapter 2 — Situation Analysis

2.1 Economic Landscape of Cybersecurity in Zambia

ICTs, particularly Broadband technology, are a key contributor to economic growth at various levels. The deployment of such technologies improve productivity by facilitating the adoption of more efficient communication, resource sharing which consequently improve business processes. Further, extensive deployment of broadband accelerates innovation by introducing new consumer applications and services.

According to a recent report by the World Bank on the impact of broadband on the economy, ICTs contribute 5-10% to the GDPs of countries mostly in developing countries. Further, it is estimated that for low and middle income economies, a 10 % increase in broadband penetration yields an additional 1.38% in GDP growth. The economic landscape is affected by various factors as highlighted below.

2.1.1 Globalisation

The increase in the use of the internet has enhanced globalisation leading to increased social and economic interconnectedness. As a result of globalisation, there has been growth in the information society which has consequently led to increased e-commerce, e-government, innovation and access to information across borders. Due to the borderless nature of cyberspace, the area of cyber-attacks and cybercrimes has greatly increased and citizens are susceptible to cybercrimes owing to the increased use of ICTs.

2.1.2 Digital Inclusion

Zambia's economy has been on the positive trajectory for the last eighteen (18) years leading to improved income levels for an expanded population. This has increased the up-take of ICTs by the larger part of the population in virtually all sectors of the economy. Similarly, the Government has taken significant strides in developing and investing in ICT infrastructure such as the construction of communication towers in underserved and unserved areas. This has led to more and more people being connected to the information networks and potentially be exposed to cyber threats.

2.1.3 E-services

E-services are commercial or non-commercial in nature. There are several such services in the private sector but currently Government provides e-services to the public which include e-tax, e-pensions and e-health. According to the Seventh National Development Plan (7NDP), more than 142 e-services will be provided to the public by 2021. The reliance on modern technologies to deliver services constantly exposes citizen's personal data and country's Critical Information Infrastructure (CII) which includes power, water, fuel, communication, factories or commercial assets that are essential for the functioning of our society and economy, to cyber-attacks.

2.1.4 E-commerce

E-commerce transcends international borders. It is estimated that global retail ecommerce is worth $28 trillion. In Zambia, the number of people using the internet to purchase goods and services from within and abroad is growing and set to continue even at a faster rate as more and more people get connected to the internet due to the enabling legislations Government has put in place.

Together with investment in communications infrastructure, Government's overall goal has been to facilitate digital financial inclusion and thereby facilitating ecommerce. According to ZICTA's ICT Survey on access and usage of Information and Communication Technology Report of 2018 internet penetration rate in Zambia stood at 51.8% in the first quarter of 2020. The report cited the increase in internet penetration rate to an increased in the participation in e-commerce activities by Zambian citizens.

The Report also revealed that the number of internet users that used the internet to purchase goods and/or services online increased, from 84,058 individuals in 2015 to 100,092 individuals in 2018. This also translates to an increase in the number of individuals expoed to several cyber threats.

2.1.5 Digital Financial Services

The use and promotion of Digital Financial Services (DFS) has facilitated financial inclusion. According to a survey conducted by the Bank of Zambia on the State of the DFS Market in 2018, the country experienced significant growth in terms of the number of active customers, agents and DFS providers. The survey also revealed that the industry went from having only 2% active DFS accounts with four providers in 2014 to 44% active DFS accounts with 18 providers in 2018. Between December 2017 and December 2018, active DFS accounts grew by 89%. Responding to the rise in active customers, the number of active agents grew from 22,965 to 46,747 in the same period.

In 2019, Mobile Money transactions in Zambia stood at more than ZMW12 billion. With the launch of the Financial Inclusion Strategy, it is envisaged that DFS would become universally accessible.

Further, according to the ICT survey of 2018, at least 48.9% of households across the country used digital financial services with more than 70% of them able to receive and send money. There has been a rise in the use of DFS leading to a corresponding rise in fraudulent activities. For instance in 2019, ZICTA received 791 consumer complaints, the majority of which were associated to DFS representing 64% of the total complaints received.

2.2 Technological Development

The pace of technological development is remarkably fast. The ICT landscape is fast-evolving as devices and services proliferate, broadband connectivity has become increasingly pervasive, and the hyper-connected world of the 'Internet of Things' is quickly becoming a reality. At the core of this phenomenal transformation is Mobile technology capable of delivering high speed internet. The expanding mobile broadband is responsible for connecting the large population of today's world to a wide range of online resources and services leading to cybersecurity related issues.

2.2.1 Access to ICT

Globally, mobile subscribers stood at nearly 67% as at the end of 2019, while Zambia had a penetration rate of 95.4% mobile subscriptions based on the number of Subscriber Identification Module (SIM) cards purchased by consumers as at first quarter of 2020. Zambia, like the rest of the world, is increasingly reliant and dependent on ICTs. The increase in connected devices and the amount of data generated and downloaded has increased dramatically leading to cybersecurity related issues about privacy and data protection among other things, for the users.

The increase in the number of people connected to the internet has also increased the number of active users of social media platforms such as WhatsApp and Facebook which has also led to increase in the number of people causing harm to others on these platforms. These people are using these platforms to steal identities and impersonate others, cyber bully, transmit pornographic content, perpetrate hate speech and insult, abuse, falsely accuse and defraud others. Avid users of ICTs that include children and young adults have become primarily vulnerable to such vices. This emerging digital culture is placing the nation's cultural, social and economic wellbeing at risk.

2.2.2 Technological Trends

It is projected that in the near future key developments will include artificial intelligence, machine learning, machine-to-machine (M2M) infrastructure and Internet of Things (IoT). This will facilitate the development of smart homes, buildings and cities. It is further estimated that future network traffic will increasingly be driven by M2M traffic generated by billions of connected devices, products and sensors with M2M communications over mobile cellular networks already emerging as the fastest-growing ICT service in terms of traffic. Many of these applications have been made possible by 4G (Long Term Evolution (LTE) - Advanced and 5G technology. One key feature of 5G, the enhanced Mobile Broadband (eMBB) which supports the internet of everything, will bring about new and advanced cybersecurity threats.

2.2.3 Technological Innovations

Broadband expansion and availability across the world has inspired innovations in the areas of machine learning, cloud computing, over the top services and big data management which is expected to shape the broader telecommunications sector. Notably, advancements in wearable technologies and use of crypto currency is expected to increase leading to an upsurge in a cybercrime known as ransomware.

2.3 Legal and Regulatory Framework

2.3.1 Legal Framework

Currently, the two principal legislation governing cybersecurity are the Electronic Transactions and Communications Act No. 21 of 2009 and the Information and Communications Technology Act No. 15 of 2009. While the ECT Act defines the rules and procedures on matters related to cybersecurity, it does not adequately deal with the many dimensions of cybersecurity nor cover the spectrum of emerging cybercrimes. This has necessitated the need for the review of the ECT Act to address current lacunas.

The ECT Act no 21 of 2009 Act does provide some procedures on cryptographic controls, this provision is implemented ad-hoc and where required, particularly in financial institutions.

The ECT Act does not promote the disclosure of vulnerabilities and threats encountered by critical infrastructure, such as banks, but whether organisations actually engage in reporting is difficult to determine. There is no mechanism that enables the disclosure of vulnerability information for analysis and decision making in the Act.

2.3.2 Licensing Regime

Zambia's liberalisation of the ICT sector brought about many changes in the internet service provision and mobile telecommunication industry. The country has at present, a total of 89 licensees in the ICT sector divided as follows: 51 Network Licensees of which three (03) are in the international market segment, 38 in the national market segment, four (04) in the provincial market segment and 6 in the district market segment, 32 service without a network licensee of which 27 are in the national market segment, two (02) in the provincial market segment and three (03) in the district Market segment and six (06) service without a network licensees in the National Market segment.

The country has more than 14,000 kilometres of optic fibre offering high speed connectivity and connecting Zambia to more than six different routes. Each major Network Licence operator terminates its traffic using its own gateway. When there is a cyber-attack on such a network arrangement, the response might be uncoordinated and lack resilience, therefore, posing a higher cyber-security risk in that it is difficult to monitor and defend the cyber space.

2.3.3 Regulatory Overlaps

The Banking, Broadcasting and Mobile Network Money Services have converged on the ICT devices, platforms and infrastructure in the form of Smart phones, Smart Televisions and mobile money. The convergence has created an overlap in duties among the Financial, Broadcasting and the ICT Regulator. The overlapping of roles is due to the convergence of radio, television and financial transactions which poses cyber threats as Regulators are limited by their respective mandates.

2.3.4 Processes and Standards

The process of acquisition, development and use of ICT tools is often a source of cybersecurity concern. A number of ICT security, procurement and software development standards have been adopted across Government and the private sector. However, the public sector does not have appropriate standards to guide the development and use of software designed to forestall cyber threats.

2.3.5 International Conventions and Protocols

As a result of the borderless nature of cybersecurity, the policing and safeguarding of the Cyber space almost often requires International Cooperation to enforce. It is for this reason that globally and regionally, countries have adopted to come together to forge cooperation in the area of cybersecurity. Notable among these international conventions and guidelines are the 2014 African Union (AU) Convention of Cybersecurity and Personal Data Protection that Zambia is a signatory to and needs to ratify.

The AU Convention on Cybersecurity and Data Protection aims at defining the objectives and broad orientation of the information society in Africa and strengthens existing legislation on Information and Communications Technologies of Member States and Regional Economic Communities. The goal of the Convention is to address the need for harmonised legislation in the area of cybersecurity in Africa and establish mechanisms of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use of that data.

2.4 Institutional Framework

Zambia Information and Communications Technology Authority (ZICTA) is currently responsible for matters related to cybersecurity. The Zambia Computer Incidence Response Team (ZM-CIRT) under ZICTA is one of the major frameworks that deal with cybersecurity incidents in Zambia. The ZM-CIRT supports Law Enforcement Agencies conducts digital forensics to aid in investigations and detect and respond to cyber related attacks. Further in 2014, ZICTA partnered with the Zambia Police Service to establish the Zambia Digital Forensics Laboratory to aid in digital investigations.

Additionally, the country's CIIs in different sectors are beyond ZICTA's mandate and there are no sector specific Computer Incident Response Teams (CIRTs) to enhance the detection of cyber threats and cyber incidences.

2.5 Environmental Factors

Environmental factors such as climate change inherently raise the number of environmental crises including droughts, floods, and pandemics. These occurrences have the potential to disrupt the provision of critical ICT services and also affect national security. A disastrous weather event can affect signalling on terrestrial as well as satellite communication networks and shut down critical electronic and digital systems.

2.6 Digital Literacy, Skills and Education

A poor cybersecurity culture among citizens, puts both the individual and the country at very high risk of cyber-attack. Studies have shown that the greatest security vulnerability within an organisation or a country is often the inadequate knowledge by individuals about the potential risks of their actions or lack thereof. For instance, the common habit of sharing of Personal Identification Numbers (PINs) and passwords voluntarily with strangers has led to loss of money.

Digital literacy and ICT education can guarantee a good cybersecurity culture and awareness. Zambia unfortunately has very low digital literacy levels especially among the old, young children, women and persons with disabilities. Despite ICT having been introduced as a mandatory subject in schools, most schools do not have enough nor appropriate ICT equipment and materials to cater for the demands of an often large population of learners.

Chapter 3 — Vision, Rationale and Guiding Principles

3.1 Vision

"A secure and resilient Zambian cyberspace by 2030"

3.2 Rationale

The country needs to have a National Cybersecurity Policy in place in order to protect its cyberspace. This is because cyberspace is central to the governance of our nation and thus essential to our socio-economic wellbeing and national security. There are a number of sectors in the economy that are heavily dependent on cyberspace for operations.
Further, the development of the Policy has been necessitated by the need to:

1. Address the inadequate cybersecurity provisions in the National ICT Policy of 2006;
2. Protect critical information infrastructure in both public and private sectors;
3. Develop a coordinated cybersecurity governance structure;
4. Provide mechanisms to ensure a safe and secure cyber environment;
5. Enhance the cybersecurity culture; and
6. Promote effective international cooperation on cybersecurity matters.

The National Cybersecurity Policy would foster the defence of a resilient Zambian cyberspace.

3.3 Guiding Principles

The following principles will guide the implementation of the National Cybersecurity Policy:

Coordination	This Policy shall promote coordination in cybersecurity defence and other operations among relevant stakeholders;
Inclusive Stakeholder Participation	Public-Private collaboration shall be the basis for the implementation of this Policy;
Accountability	Professionalism and responsible use of ICTs are cardinal to the implementation of cybersecurity in Zambia;
Human dignity, equity and social justice	The rights of individuals should be respected in implementing the Policy;
Patriotism	It is the duty of every Zambian citizen to defend the country;
Good governance and integrity	Good governance shall enhance the provision for a coordinated approach in addressing cybersecurity in Zambia.

Chapter 4 — Policy Objectives and Measures

4.1 Overall Objective

To transform the cyberspace in Zambia into a safer environment in order to fully realise the social, economic and strategic benefits of using ICTs.

4.2 Specific Objectives and Measures

4.2.1 Objective 1:

To secure Zambia's critical information infrastructure to enhance cyber resilience.

Measure

Enhance mechanisms to ensure that Zambia's critical information infrastructure is adequately protected.

4.2.2 Objective 2:

To develop a coordinated governance framework and set the agenda for cybersecurity in order to ensure a safe and secure cyberspace.

Measures

a. Enhance the legal and regulatory framework for secure digital identity management
b. Develop mechanisms to ensure compliance with cybersecurity standards
c. Promote a multi-sectoral approach to cybersecurity
d. Enhance investment in cybersecurity
e. Develop a coordinated framework for child online protection.

4.2.3 Objective 3:

To promote international cooperation in order to effectively deal with cybersecurity incidents.

Measure

Enhance collaboration with international stakeholders and engage with other countries and international institutions on matters relating to cybersecurity.

4.2.4 Objective 4:

To promote cybersecurity education and develop requisite skills in order to attain a culture of cybersecurity.

Measures

a. Develop a mechanism to integrate cybersecurity in all education and training programmes.
b. Enhance the development of cybersecurity awareness programmes.
c. Develop mechanisms to improve cybersecurity capabilities.

4.2.5 Objective 5:

To promote Research and Development in cybersecurity in order to reduce the reliance on foreign cybersecurity solutions.

Measures

a. Develop indigenous cybersecurity capabilities and technologies.
b. Develop research and development programmes relating to cybersecurity.
c. Establish institutional collaborations with the relevant institutions to conduct research in cybersecurity

Chapter 5 — Implementation Framework

5.1 Institutional Framework

Attaining the objectives of this Policy will take a multi-sectoral approach. The Ministry of Transport and Communications will take the leading role in the coordination and implementation of this Policy. The Policy recognises the roles of the following institutions:

Institutions	Roles
Ministry responsible for Defence	• Participate in the country's defence against cyber warfare
Ministry responsible for Home Affairs	• Prevention, investigation and combating cybercrimes/cyber incidents • Ensure compliance to cybersecurity regulations
Ministry responsible for Finance	• Resource mobilisation to support cybersecurity operations and management
Ministry responsible for Justice	• Align and harmonise all relevant laws pertaining to cybersecurity • Facilitate prosecution and all court processes related to cybercrimes in accordance with the applicable laws
Ministry responsible for Foreign Affairs	• Facilitate signing, accession and ratification of appropriate cybersecurity conventions and treaties. • Facilitate international cooperation in cybersecurity.
Ministry responsible for National Development Planning	• Evaluate cybersecurity projects earmarked for investments • Provide guidance on long term plans for cybersecurity management.
Ministry responsible for Commerce, Trade and Industry	• Promote a safe and secure environment in order to enhance e-commerce.
Ministry responsible for Information and Broadcasting Services	• Undertake awareness programmes on cybersecurity
Ministry responsible for Higher Education	• Incorporate cybersecurity education and awareness in the curriculum. • Promote research and development in cybersecurity
Ministry responsible for General Education	• Incorporate cybersecurity education and awareness in the curriculum.
Ministry responsible for Housing and Infrastructure Development	• Facilitate construction of relevant infrastructure for cybersecurity.
Zambia Information and Communications Technology AuthorityCommunications Technology Authority	• To regulate and carry out all functions related to cybersecurity and cybercrime
Smart Zambia Institute	• Promote cybersecurity in the provision of Government electronic services
Disaster Management and Mitigation Unit	• Coordinate responses to disasters emanating from cyber-attacks.
Private Sector	• Support initiatives towards enhancing cybersecurity resilience • Ensure preparedness to respond to cyber threats
The Individual	• Enhance awareness of cybersecurity threats and adopt appropriate cybersecurity safeguards.

Government will establish a National Cybersecurity Advisory and Coordinating Council (NCACC) comprising key stakeholders who will be responsible for overseeing, coordinating and enhance collaboration among security wings.

The institution responsible for Cybersecurity shall perform among others, the following functions;

- Carry out all activities aimed at combating of cybersecurity and cybercrime;
- Recommend emergency cybersecurity measures to the National Cybersecurity and Coordinating Council;
- Provide strategic intelligence operations to strengthen cybersecurity in Zambia;
- Undertake research and development in cybersecurity; and
- Promote cybersecurity awareness, education and training.

5.2 Legal Framework

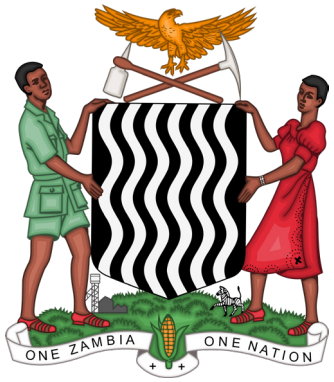
Government will review the ECT Act in order to introduce the Cybersecurity and Cybercrimes Act to adequately address cybersecurity and cybercrimes. The revision will ensure that Government promulgates various regulations for identification and classification of critical information infrastructure and regulations that require organisations to have specific policies and procedures for notifying the national CIRT of Cybersecurity incidents.

5.3 Resource Mobilisation

Government will mobilise finances for the implementation of this Policy from domestic revenues, bilateral and multilateral Cooperating Partners and the Private Sector. Through this Policy, Government will vigorously pursue innovative resource mobilisation using the Public Private Partnerships (PPP) framework.

5.4 Monitoring and Evaluation

The Ministry will establish a sector wide Monitoring and Evaluation system that will provide evidence for assessing the impact of the implementation of this Policy. Due to the fast changing nature of ICTs, regular Policy reviews will be conducted to ensure responsiveness to these changes. The Policy will also be subjected to a midterm review after 5 years and a comprehensive evaluation after 10 years of implementation.



Republic of Zambia

Ministry of Transport and Communications

www.mtc.gov.zm