NATIONAL CYBERSECURITY STRATEGY

(FINAL DRAFT)

Version 5

TABLE OF CONTENTS

ACRONYMS

CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
ICT	Information and Communications Technology
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol version 6
ISP	Internet Service Provider
LTE	Long-Term Evolutions
M&E	Monitoring and Evaluation
MDF	Malawi Defence Forces
MACRA	Malawi Communications Regulatory Authority
MGDS	Malawi Growth and Development Strategy
MICT	Ministry of Information and Communications TechnologyICT
NCS	National Cybersecurity Strategy
SOP	Standard Operating Procedures
R&D	Research and Development
WiMax	Worldwide Interoperability for Microwave Access

EXECUTIVE SUMMARY

Communication services in Malawi have been governed by the Communications Act (1998) which was developed during the era of second generation (2G) technologies. Since then, Malawi has seen the growth of access and usage of ICT services, including an increasing number of online transactions for services. The increasing demand for the ICT applications and services coupled with the provision of high-capacity fibre backbone connectivity across the nation has resulted in the creation of substantial opportunities for further growth in the ICT sector. It is also expected that these developments will drive significant socio-economic growth in Malawi. Consequently, and in an effort to create a conducive environment for the sustained growth and use of ICTs in Malawi, as well as address the threats that come with increased adoption of ICTs, the Government of Malawi undertook a review of existing legislation and developed the Communications Act (2016) and the Electronic Transactions & Cyber Security Act (2016).

ICT has become a critical driver for socio-economic development, with the deployment and adoption of ICTs across the nation resulting in noteworthy improvements in all aspects of lives and institutional operations in the nation. However, a number of risks and threats exist or have emerged that restrict the smooth operation and resilience of ICT systems, and consequently the socio-economic development of the nation. This Strategy aims to provide a national framework for ensuring secure, safe and resilient cyberspace, as well as fostering trust and confidence in cyberspace by Malawians, by describing the high level strategic goals and specific objectives that provide the basis of the nation's direction with respect to cybersecurity, and establishes actions that need to be taken.

Chapter 1 of the strategy provides an introduction to cybersecurity in Malawi while chapter 2 details the guiding principles upon which the Strategy is built on, and which will underpin the implementation of the Strategy. Chapter 3 outlines the core components of the National Strategy including the vision mission statement, high-level strategic goals and specific objectives. It further describes the various actions necessary for achieving the Specific objectives and strategic goals of the strategy. Chapter 4 describes the roles and responsibilities of the key stakeholders in the implementation of the strategy and further proposes an approach for monitoring and evaluating the implementation of the strategy. The implementation logical

frameworks for the strategy which provide details on *Deliverables,* Key *Performance Indicators (KPI)*, *Timeframes*, *Lead Organisations* and *Funding* options are described in the Appendix.

This NCS Strategy therefore outlines the Government of Malawi's approach to ensuring a safe and secure cyberspace that can be fully leveraged by citizens and institutions. Consequently, driving further growth of the ICT sector, as well as socio-economic development across Malawi.

1 INTRODUCTION

1.1 Background

Major reforms in the ICT Sector of Malawi go as far back as the 1990s with the advent of sector liberalisation through the separation and commercialisation of the then incumbent Telecommunications operator, Malawi Posts and Telecommunications Corporation (MPTC) into the Malawi Telecommunications Limited (MTL) and Malawi Posts Corporation (MPC). Subsequent major reforms include the implementation of the Communications Sector Policy (1998) and the Communications Act (1998) that led to the establishment of the Malawi Communications Regulatory Authority (MACRA). Due to advances in technology over the years, the Communications Act (1998) was reviewed to the Communications Act (2016) and also the Electronic Transactions and Cyber Security Act (2016) were enacted. These are the two current legislations for the sector.

Currently, the mobile penetration rate in Malawi is quite low in comparison to the average African penetration rates, highlighting the tremendous potential for further growth in Malawi. The broadband access prices in Malawi are among the highest in the region due to high cost and limited availability of international bandwidth. However, the internet sector has about 50 licensed ISPs out of which only 20% are active.

The mobile penetration and broadband are expected to grow exponentially over the next couple of years. Since, the current mobile market in Malawi is a duopoly, the government of Malawi has introduced a converged licensing regime in an effort to encourage further market competition and growth. It is expected that the converged licensing regimes will introduce new entrants into the sector and enhance competition resulting in lower prices. In addition, service providers in Malawi have launched 3G services, invested in LTE infrastructure or continued to extend their WIMAX wireless broadband networks. Furthermore, Malawi gained access to international submarine cables recently following the completion of a transit link via neighbouring countries and is currently deploying a national fibre backbone.

As a result of these recent developments within the sector, as well as the high potential for further rapid proliferation of ICTs within Malawi, it is evident that Malawians will increasingly get connected to the Internet and use ICTs overtime. This increased connectivity and use of ICT's

come with increased threats to activities of businesses and people in Malawi. If Malawi is to fully leverage ICTs to spur socio-economic development of the nation, it has to be ready and capable of addressing these threats.

NCS 2017-2021 sets out a multi-stakeholder framework for ensuring Malawians can access and use cyberspace with trust and confidence, and ensuring the nation responds to threats to ICT systems and services in a coherent and effective manner.

1.2 Situational Analysis

1.2.1 National Development and the Role of ICT

The Government of Malawi in its last development and growth strategy (MGDS 2011 -2016) recognized how critical a well-developed ICT system is in the development of Malawi. The Government embarked on implementing a number of strategies resulting in a number of desired outcomes including improved ICT broadband infrastructure; increased access and usage to ICT services; improved postal and broadcasting services; improved ICT governance; and enhanced ICT capacity for the general public. This is consistent with the Government's current overarching Policy Goal for ICTs in Malawi, as described within the National ICT Policy (2013) which is "to contribute to socio-economic development through maximum integration of ICT in all sectors and the provision of ICT services to the rural areas".

The development of the MGDS follows a phased approach to address the ICT development needs of the country in support of the prevailing policies and the legal framework. The MGDS was developed to be the overarching operational medium-term strategy for Malawi in the attainment of its set vision. The main thrust of the MGDS is to create wealth through sustainable economic growth and infrastructure development as a means of achieving poverty reduction. The MGDS I was developed to lay the framework while MGDS II was tasked with putting in place the operational mechanism. The NCS therefore feeds into MGDS II as well as the plans for development of MGDS III thereby addressing Government goals of universal ICT access within a safe and secure operational environment.

This policy direction is quite consistent with global research studies and evidence that clearly demonstrates the connection between ICT adoption and usage of ICT services with national GDP growth. In fact, the World Bank has demonstrated the greater development impact of broadband specifically on emerging economies as compared to high-income countries.

Currently, Malawi's broadband penetration has risen from 6% in 2013 to around 17.1% in 2016, which is relatively low compared to other Southern African Development Community (SADC) countries and the rest of the world. However, with the rapid development of the ICT sector, the Government of Malawi through the Malawi Growth and Development Strategy (MGDS 2011-2016), recognizes the potential broadband growth which puts the users of ICT services at a cyber risk. Thus, the Government of Malawi needs to be prepared and deploy effective strategies or measures to create a conducive environment that builds trust and confidence in the use of ICTs by Malawian businesses and citizens.

1.2.2 Cybercrime in Malawi

The Government of Malawi recognizes that high levels of crime across the nation results in significant socio-economic damage and nullifies significant developmental activities. In fact, in the National ICT Policy (2013), the Government set out to establish sufficient national capacity to deal with national security, the violation of human rights, and the undesirable impacts of ICTs such as the privacy violations, cybercrimes, digital frauds and terrorism. Despite the government's position, and like other nations across the world, cybercrime continues to be a real threat and facet of life in Malawi. Cyber criminals continue to commit cybercrimes of larger scales and sophistication across various countries, including Malawi. Many of these cyber criminals seek to make use of confidential and sensitive information and usually have detrimental effects on individuals, businesses and government institutions in the country. Consistent with global trends, a major sector targeted by cyber criminals in Malawi is the financial sector. Other key cybercrime incidents that have been observed in the country include identity theft, various email scams, distribution of compromising images, attacks on computer data and systems. Therefore, it is critical that Malawi develops a strategy that protects its citizens and institutions from these cyber criminals and enhances the nation's ability to detect, prosecute and prevent cybercrimes in Malawi.

The high levels of ICT access and usage in the country coupled with the absence of specific legislation dealing with cyber security issues in Malawi proved a big challenge in the fight against common forms of cybercrime namely—*true cybercrimes*, which are committed against the confidentiality, integrity and availability of computers, computer systems and networks, hacking, malware and website defacement among others. Secondly, *traditional crimes*, which

are committed through the instrumentality of computers, computer systems and data e.g. child pornography, sexual harassment, fraud, forgery, crime recorded and posted online and others.

However, the enactment of the Electronic Transactions & Cyber Security Act (2016) has provided a platform to harness all the efforts that were being hampered by lack of appropriate legislation. Malawi is also benefiting from regional initiatives and harmonization of strategies to provide a model standard for the region.

1.2.3 Malawi's Cybersecurity Related Activities

Understanding the current cybersecurity-related activities of Malawi is critical to ensuring the effective cooperation between Malawi's stakeholders and their cybersecurity-related mandates and activities. Therefore, this Strategy considers the various functions and activities of the different stakeholders in Malawi relating to cybersecurity. Noteworthy cybersecurity-related activities undertaken in Malawi over the past year include the recent promulgation of the Electronic Transactions and Cyber Security Act (2016) and the development of this National Cybersecurity Strategy. The recently promulgated Electronic Transactions and Cyber Security Act (2016) address a number of ICT security issues like cybercrime, data protection, and privacy among others. For instance, the Electronic-Transactions and Cyber Security Act (2016) will enable citizens to undertake various electronic transactions with the full protection of the law, as well as ensure citizens are protected from computer related harms like cybercrimes, viruses and hacks. Part 6 of the Electronic-Transactions and Cyber Security Act (2016) provides details of offences; Clause 87, for instance, addresses events where an individual knowingly introduces or spreads a software code that damages computer, computer system or network. Other issues addressed in the Act include cryptography, Country Code Top Level Domain (ccTLD), the establishment of the Malawi National CERT and the appointment of cyber inspectors.

However, efforts to address challenges within the cyberspace in Malawi were fragmented due to the absence of a coordinated strategic approach by all key stakeholders. The NCS will therefore provide a link among all these stakeholders to provide effective solutions to the identified challenges. The NCS as an overarching strategy provides a platform for: the Ministry of Justice to deal with the legal issues related to the cyberspace in conjunction with all law enforcement

agencies; the regulatory authorities to review the effectiveness of the legal and regulatory framework; and the academia to review the curricula and offer training suited to the trends in addressing challenges in the cyberspace.

The extent of cyber issues entails generic actions to specific sectors that eventually feeds into the national strategy. For instance the. banking sector has embarked on sector specific training to address the needs of the banks, likewise the academia has also incorporated various courses for cybersecurity in order to enhance the level of knowledge and awareness for cybersecurity.

1.2.4 Linkages with other National Policies and Programmes

The National Cybersecurity Strategy is aligned with and will complement the following Government of Malawi policies and legislations:

- Science and Technology Policy (2002)
- The National ICT Policy (2013)
- The National ICT Master Plan (2014 – 2031)
- Electronic Transactions and Cyber Security Act (2016)
- Malawi Growth and Development Strategy II (2011 -2016)
- Vision 2020
- Communications Act (2016)

Additionally, the NCS will be reviewed regularly to ensure that it continues to be aligned to future national strategies/plans.

2 GUIDING PRINCIPLES

The National Cybersecurity Strategy is built on the following Guiding Principles:

i. **Risk-based approach**: The Cybersecurity Strategy will ensure that a risk-based approach is adopted by the private sector, the government, academia and civil society in assessing and responding to cyber-related threats or issues.

ii. **Multi-stakeholder approach**: The Cybersecurity Strategy will seek to enhance the effectiveness of all key stakeholders in improving the cybersecurity posture of Malawi by recognizing the various roles and responsibilities of different stakeholders and promoting national cooperation and coordination for cybersecurity-related activities amongst stakeholders.

iii. **External Co-operation**: The Strategy will also promote bilateral, regional and international cooperation, recognizing the borderless nature of cyberspace.

iv. **Respect for the rule of law and human rights**: The Cybersecurity Strategy is aligned with the laws in force in Malawi. It is also aimed at facilitating the promotion, protection and enjoyment of fundamental human rights and freedoms of Malawian citizens.

v. **Capacity development**: The Cybersecurity Strategy will seek to enable the continuous development of the Malawi's capacity to address fast changing cybersecurity issues and developments.

vi. **Socio-economic development**: The National Cybersecurity Strategy will ensure cyberspace is fully leveraged by Malawi to spur broader socio-economic development, facilitate sustainable socio-economic development across the entire nation.

vii. **Addressing Cybercrime**: The National Cybersecurity Strategy will promote and facilitate both individual and collective action in tackling cybercrime, recognizing both the individual responsibility and collective responsibility in taking steps in combating cybercrime.

3 THE NATIONAL CYBERSECURITY STRATEGY OF MALAWI

This section of the Strategy articulates Malawi's Vision and Mission Statements for Cybersecurity as well as the core elements of Malawi's approach to improving the cybersecurity posture.

3.1 Vision

Malawi's vision for 2021 is:

"A nation with a secure, trusted, resilient and safe cyberspace that promotes a knowledge-based society and socio-economic development"

3.2 Mission

Malawi's mission is:

"To develop and deliver effective cybersecurity capacity, services and infrastructure that instills confidence in cyberspace"

3.3 Strategic Goals

To achieve the abovementioned Vision, the Government of Malawi will work to achieve the following Seven Strategic Goals:

1. Identify and manage the critical information infrastructure of Malawi
2. Develop and enhance cybersecurity-related capacity, infrastructure, legal, regulatory and other related frameworks.
3. Promote awareness, information sharing and collaboration on cyber security.
4. Enable and continuously improve the safety of vulnerable groups[1] in cyberspace, especially the safety of children.
5. Enhance and coordinate the fight against all forms of cybercrime
6. Promote the use of cyberspace to drive social and economic development

[1] Where vulnerability is the degree to which a population or individual is unable to anticipate, cope with, resist and recover from the impacts of threats resulting from either the environment or from personal circumstances

The following section details the Specific Objectives and Actions required to achieve the abovementioned Strategic Goals of the Strategy.

3.4 Specific Objectives and Actions

I. Strategic Goal (i): Identify and manage the Critical Information Infrastructure of Malawi

Protecting the information infrastructure of Malawi is of critical to the Government of Malawi, especially as successful cyber attacks on them will have severe impacts on the country. These impacts could include destabilization of Malawi's economy and stability or reputational damages to individuals. Therefore, it is vital that Malawi prioritizes the cybersecurity of its critical information infrastructures (CIIs) which are key for the provision of essential services to Malawi by ensuring these CIIs are secure and resilient. The protection of Malawi's information infrastructure including CIIs necessitates collaboration of all relevant stakeholders including public and private institutions that own or operate the information infrastructure which supports the well-functioning of the Malawian society. Consequently, the Government of Malawi will work with all relevant stakeholders to identify and understand the vulnerabilities and levels of cybersecurity of Malawi's information infrastructure, especially CIIs. The Government will also work with relevant stakeholders to establish measures that will address current and future cyber threats and risks to the national information infrastructure, and drive improvements where necessary.

3.4.1 Specific Objective 1: Identify and protect the Critical Information Infrastructure of Malawi.

Actions:

3.4.1.1 Establish a National CII Register

3.4.1.2 Develop a National CII Governance Framework which provides details on CII protection procedures and processes

3.4.1.3 Establish a National Risk Register and Regulations and/or Guidelines that promote continuous risk assessment and management across CIIs in Malawi

3.4.1.4 Establish Mandatory Equipment Specifications, Mandatory Guidelines, Regulations, Security Requirements, Procedures relating to the management of risks by CIIs

3.4.1.5 Create a National Vulnerability Register and Framework for regular vulnerability monitoring and disclosure for CII

3.4.1.6 Undertake continuous monitoring and regular testing to detect errors, vulnerabilities, and intrusions in CII

3.4.1.7 Promote and enhance regional and international cooperation in the protection of the critical information infrastructure (CII)

3.4.2 Specific Objective 2: Continuously monitor and manage cyber threats and risks to enhance incident response.

Actions:

3.4.2.1 Expedite the establishment and operationalization of a national CERT with clear processes, defined roles and responsibilities

3.4.2.2 Continuously develop the capacity of staff at Malawi National CERT to address the fast changing technical requirements, and develop abilities to actively obtain information in cyberspace, about current cyber risks and threats

3.4.2.3 Develop a national incident reporting, information sharing and coordination mechanisms to address reporting of incidents and coordination in incident response

3.4.2.4 Create and continuously update cyber security incidents register, assess incidents, and suggest measures to resolve issues and mitigate threats and risks

3.4.2.5 Specify minimum and mandatory log/register requirements necessary for dependable cyber security incident analysis

3.4.2.6 Continuously monitor, analyse and assess cyber threats and potential risks and be able to provide a real time overview of the state of cybersecurity across nation

3.4.2.7 Develop a Cybersecurity Governance Framework for defining roles and responsibilities of all stakeholders in the cybersecurity ecosystem as well as describe SOPs and Code of Conduct in responding to incidents

3.4.2.8 Establish a call center/help line for reporting incidents or seeking assistance with incidents

3.4.2.9 Develop and implement cybersecurity incident simulation scenarios and programs that can be used during the national exercises

3.4.2.10 Develop and continuously update cybersecurity contingency plans, which will include roles of the military/security forces during cyber-attacks and emergencies

3.4.2.11 Develop and test requisite crisis management measures during frequent cyber drills

3.4.2.12 Evaluate cyber drills to develop options on how to improve crisis management measures

3.4.2.13 Develop a Cyber Defence Strategy that details approaches to addressing threats to national security in cyberspace

3.4.2.14 Establish a Central Defence Command and Control Centre for cybersecurity in Malawi

II. **Strategic Goal (ii)**: **Develop and enhance cybersecurity-related capacity, infrastructure, legal, regulatory and other related frameworks**

The limitation of cybersecurity capacity, infrastructure, and other related frameworks is recognized as a key challenge for Malawi which impairs the nation's efforts in ensuring high levels of cybersecurity. Aligned to the national vision of creating information driven and knowledge based society, the Government of Malawi will seek to ensure that there is an available pool of highly skilled and knowledgeable cybersecurity professionals in Malawi. The Government will also seek to promote research and development in cybersecurity as well as create an enabling environment where innovation and creativity in cybersecurity can be fostered.

Considering that all ICT users including individuals, public or private sector are required to take necessary steps in ensuring their cybersecurity including investing in infrastructure or technology, the Government will facilitate the deployment of, and usage of requisite infrastructure/technology necessary to ensure good levels of cybersecurity nationwide.

The Government will also seek to establish and strengthen a range of cybersecurity-related frameworks which will enhance the cybersecurity of Malawi. For instance, the Government will seek to strengthen the legal and regulatory framework of Malawi to support the cybersecurity landscape and create a conducive environment for the effective use of cyberspace by individuals, the public and private sector.

3.4.3 Specific Objective 3: Strengthen Malawi's legal and regulatory frameworks to enhance cybersecurity in Malawi

Actions:

3.4.3.1 Undertake a gap analysis to identify gaps in current ICT Security Legal and Regulatory Framework and develop requisite instruments to address Gaps including issues relating to privacy and data protection.

3.4.3.2 Develop and publish a cybersecurity policy and standards consisting of general and sector-specific cybersecurity controls that would be recognized as a national standard

3.4.3.3 Create a national programme to promote the adaptation and adoption of cyber standards across government institutions and CII in Malawi

3.4.4 Specific Objective 4: Stakeholder capacity building for law enforcement and judiciary to implement cybersecurity related laws

Actions:

3.4.4.1 Identify needs and then provide training and education to develop the capacities of the law enforcement agencies, judiciary and the legal fraternity on how to interpret and enforce the policy, legal and regulatory frameworks on cybersecurity in Malawi

3.4.5 Specific objective 5: Enhance technical and procedural measures for implementing cybersecurity for CIIs

3.4.5.1 Establish mandatory and minimum technology and security requirements for CIIs

3.4.5.2 Develop a national government programme to deploy and manage government ICT infrastructure

3.4.5.3 Develop a national programme to enhance internet infrastructure development and resilience.

3.4.5.4 Develop National Contingency plans which identify emergency response asset priorities and standard operating procedures (SOPs)

3.4.5.5 Review and update the map of current emergency response assets

3.4.5.6 Ensure communication channels are deployed across emergency response functions, geographic areas of responsibility, public and private responders, and command authority.

3.4.6 Specific Objective 6: Continuously develop and enhance the cybersecurity technical capacity in Malawi

Actions:

3.4.6.1 Revise the National Research Agenda to promote R&D in cybersecurity in Malawi

3.4.6.2 Establish a National Centre of Excellence for Cybersecurity Training & Research

3.4.6.3 Review and update primary, secondary and tertiary level education curriculum to include cyber security elements

3.4.6.4 Support cybersecurity competitions and R & D projects in Universities and Schools

3.4.6.5 Support national enterprises providing cybersecurity solutions, and undertaking R & D in cybersecurity

3.4.6.6 Collaborate with universities, colleges and the private sector to create new studies and internship programs on cyber security

3.4.6.7 Collaborate with the private sector and academia to support participation of government institutions, universities, private sector in regional and international research projects and exercises relating to cybersecurity

3.4.6.8 Create standards in cybersecurity training and education

3.4.6.9 Train ICT personnel of various Government ministries and institutions on how to detect incidents, report incidents, and collaborate with the national CERT and institutions from other sectors on cybersecurity

3.4.7 Specific Objective 7: Facilitate the recruitment of, and retention of cybersecurity expertise within Malawi

Actions:

3.4.7.1 Develop National and Career Progression Policy promoting continuous training and education for Incident Response and addressing issues relating to cybersecurity

3.4.7.2 Identify the staffing requirements for Government agencies and CII operators and develop a national recruitment and retention strategy

3.4.7.3 Develop and implement cybersecurity training and capacity building training plans for Government personnel.

III. Strategic Goal (iii): Promote awareness, information sharing and collaboration on cyber security

A significant proportion of cybersecurity incidents can be prevented by being aware of, and understanding the threat. It is critical that individuals and organizations in Malawi are aware of the threat, and are taking the appropriate measures to protect themselves from cyber attacks. It is paramount that the Government of Malawi and other stakeholders aim to undertake various awareness building programmes which not only provide information and advice to individuals and organizations on how to protect themselves but also create a national cybersecurity culture and mindset.

Recognizing the shared responsibilities of various stakeholders in improving cybersecurity in Malawi, as well as the borderless nature of cyberspace, it is imperative the Government of Malawi promotes information sharing and collaboration in the nation's efforts in addressing cyber threats and cyber incidents. The Government of Malawi will seek to establish measures that promote a culture of information sharing and collaboration across all relevant stakeholders nationally, regionally or internationally.

3.4.8 Specific Objective 8: Enhance cyber security awareness across the general public and national institutions

Actions:

3.4.8.1 Undertake a nationwide assessment to determine level of awareness of cybersecurity across the nation

3.4.8.2 Develop and implement a national roadmap for improving awareness of current cyber security trends and threats

3.4.8.3 Develop and disseminate National Cybersecurity Best Practices to engrain a cybersecurity mindset in the public

3.4.8.4 Undertake mandatory training of Board Members of different organizations to enhance their understanding of cyber issues and how their organizations address these threats.

3.4.9 Specific Objective 9: Promote collaboration and information sharing on Cybersecurity.

Actions:

3.4.9.1 Create a national forum to enhance and promote information sharing and collaboration nationally on cybersecurity

3.4.9.2 Continuously update the citizens, the private sector and the public sector, on information related to cyber threats, vulnerabilities, incidents, activities across the nation to foster trust

IV. Strategic Goal (iv): Enable and continuously improve the safety of vulnerable groups in cyberspace, especially the safety of children

The Government of Malawi recognizes its responsibility in protecting vulnerable groups, especially children as they usually lack the capacity to do so themselves. For instance, children are susceptible to cyber bullying, pornography, and other harmful content, and meeting online contacts offline, sexual solicitation and grooming. Therefore, the Government will seek to ensure that vulnerable groups, especially children, use ICTs and cyberspace in a safe and responsible manner. The Government will deploy measures that ensure that vulnerable groups especially children, as well as their minders or guardians, are informed and aware of cyber threats and risks. Furthermore, it will collaborate with relevant stakeholders to develop and deploy measures and tools to protect the vulnerable and ensure they stay safe online.

3.4.10 Specific Objective 10: Ensure online safety for vulnerable groups, especially children

Actions:

3.4.10.1 Develop and disseminate online safety guidelines and best practices to protect vulnerable groups in Malawi, especially children, from cyber threats

3.4.10.2 Deploy special awareness programmes to target and inform children and other vulnerable groups about safe and responsible use of the internet

3.4.11 Specific Objective 11: Deploy tools to ensure that vulnerable groups, especially children are safe online

Actions:

3.4.11.1 Promote the deployment of technical measures or web filtering tools that prevent access to harmful content by children and other vulnerable groups

3.4.11.2 Encourage ISPs and other services providers to make their clients, especially parents and guardians aware of how to leverage available tools, technologies to manage potential risks to vulnerable groups while accessing services online

V. Strategic Goal (v): Enhance and coordinate the fight against all forms of cybercrime

It is evident that cybercrime has several detrimental effects on the Malawian nation. Some of these impacts include economic losses, reputation damage, reduced confidence in ICT services, etc. The Government of Malawi appreciates the severity of the evolving threat of cybercrime to the nation and the numerous challenges in combating cybercrime across the nation. The Government aims to enhance the detection, investigation, and prosecution of cybercrimes in Malawi. This will require Malawi to strengthen the relevant legal and regulatory frameworks relating to Cybercrime in Malawi, as well as to build the capacity of the stakeholders responsible for the detection, investigation, and prosecution of cybercrimes. The Government also recognizes the need for coordination and collaboration in the national response to cybercrime, and will develop strong partnerships to combat cybercrime.

3.4.12 Specific Objective 12: Enhance Cybercrime detection

Actions:

3.4.12.1 Establish the requisite framework to establish and operationalize a Digital Forensics Laboratory

3.4.12.2 Develop mandatory digital forensics and evidence handling courses for the judiciary, law enforcement and personnel from other related agencies involved in the detection and prosecution of cybercrime

3.4.12.3 Build and enhance capacity to detect cybercrime incidents

3.4.13 Specific Objective 13: Enhance cooperation and awareness in the fight against cybercrimes

Actions:

3.4.13.1 Develop and continuously update an information sharing, governance and collaboration framework for the fight against cybercrime which will include links that ensure direct and timely collaboration between judiciary, law enforcement and personnel from other related agencies, service providers, CII entities, Malawi CERT and other government institutions on issues that concern cybercrime and Cybersecurity

3.4.14 Specific Objective 14: Promote international collaboration in the fight against cybercrime

Actions:

3.4.14.1 Strengthen collaboration with regional, international states and partners in combating cybercrime through treaties, conventions (e.g. Budapest) and bilateral agreements, especially through frameworks such as the 24/7 cybercrime Network, mutual legal assistance frameworks, etc.

3.4.14.2 Develop a clear plan that outlines how to manage international collaboration across multiple strategy areas such as law enforcement, incidence response, research and innovation in cybersecurity.

3.4.14.3 Subscribe to and participate in all relevant regional and international forums on cybersecurity.

VI. Strategic Goal (vi): Promote use of secure cyberspace to drive social and economic development

The Government of Malawi recognizes the multiplier effect of the cyberspace on several aspects of its society, including social and economic development. In fact, with more and more individuals and organizations adopting and utilizing ICT technologies and applications, there is extensive evidence that illustrates the positive impacts of ICTs including cyberspace. The Government seeks to create a secure and reliable environment which facilitates the secure use of cyberspace, promotes trust in cyberspace, increased usage of e-government and e-

commerce services, and consequently driving further social and economic development in Malawi.

3.4.15 Specific Objective 15: Cooperate with the private sector to ensure that cyberspace, reliably and securely, supports information sharing, R&D, and entrepreneurship

Actions:

3.4.15.1 Undertake the transition from IPV4 to IPV6 protocol and disseminate information on the benefits of the transition, especially IPV6 security features relating to confidentiality, authentication and data integrity

3.4.16 Specific Objective 16: Foster trust and confidence in cyberspace, especially in applications relating to e-government and e-commerce.

Actions:

3.4.16.1 Create, and continuously update the general public and public sector on how cyberspace is securely used in Malawi to deliver e-government and e-commerce services in Malawi, highlighting the various security features deployed to foster trust

3.4.16.2 Encourage the use of Public Key Infrastructure (PKI) for transactions to/from Government Ministries, Departments and Agencies to enhance high cybersecurity levels and trust in delivering public services.

3.4.16.3 Appoint cybersecurity inspectors whom among other duties will serve as focal points of contacts to support small and medium enterprises in addressing cybersecurity needs and method of mitigating cyber threats.

4 INSTITUTIONAL FRAMEWORK

4.1 Roles and Responsibilities

The section below describes the roles and responsibilities of key actors involved in the implementation of the strategy:

4.1.1 Office of the President

The Office of the President's will champion cybersecurity in Malawi and will provide support and leadership at the executive level to ensure the successful implementation of the National Cybersecurity Strategy of Malawi.

4.1.2 Ministry of ICT

The Ministry of ICT will be responsible for creating a conducive legal and regulatory environment for the safe use of ICTs and confidence in cyberspace, by developing relevant policies, laws, and regulations that enable the smooth functioning of the ICT sector of Malawi.

4.1.3 Malawi Communications Regulatory Authority (MACRA)

The Malawi Communications Regulatory Authority (MACRA) will be responsible for leading, planning and coordinating the implementation of the National Cybersecurity Strategy through collaboration with other stakeholders. MACRA will through CERT, continuously monitor the cyberspace to provide pro-active and reactive responses to cyber threats and risks.

MACRA provides regulatory oversight of the ICT sector of Malawi and ensures compliance to relevant cybersecurity-related frameworks within the ICT sector. MACRA will also host the Malawi CERT.

4.1.4 Ministry of Justice and Constitutional Affairs

The Ministry of Justice will lead in the prosecution of cybercrime.

4.1.5 Ministry of National Defence & Ministry of Home Affairs and Internal Security

These Ministries will be responsible for setting the policy to guide the implementing agencies i.e. Malawi Defence Force and Malawi Police Service respectively to undertake their cyber-related activities in line with the policy.

4.1.6 Malawi Police Service (MPS) and other law enforcement agencies

The Malawi Police Service (MPS) and other law enforcement agencies will be responsible for the investigation and enforcement of cybercrimes in Malawi. They will also play a vital role in collaborating with national and international stakeholders and law enforcement agencies in combating cybercrime.

4.1.7 Malawi Defence Force

The Malawi Defence Force, in collaboration with the Malawi CERT will continuously monitor the cyberspace sphere to identify and address cyber threats and risks to the National Security of Malawi. They will also work with other security forces and stakeholders to safeguard and combat cyber-terrorism and maintain law and order during nationwide incidents or emergencies.

4.1.8 Critical Information Infrastructure (CII) Owners and Operators

CII owners and/or operators in Malawi will be responsible for protecting their infrastructure from cyber threats and vulnerabilities. To this end, they will ensure that various mitigation measures are implemented to protect the CII. They will also be responsible for ensuring that they comply with various cybersecurity-related frameworks in force in Malawi.

4.1.9 The Academia

The Academia in Malawi will play a key role in the nation's efforts in developing capacity and expertise in cybersecurity to address Malawi's requirements for skilled and knowledgeable cybersecurity professionals of Malawi, at present and in the future. The Academia will also play a key role in undertaking cybersecurity-related R&D.

4.1.10 Civil Society

The Civil Society of Malawi will work with other stakeholders to promote effective engagement, promote transparency and accountability of the public and private sector institutions, and strengthen knowledge and awareness of cyber security related issues across Malawi.

4.1.11 Private Sector

The Private Sector will be responsible for protecting the data, services and systems they own, provide and operate respectively, and as such will be responsible for ensuring their compliance with national laws, policies, standards, procedures and frameworks relating to cybersecurity.

4.1.12 Citizens

The citizens will be expected to take appropriate steps in order to safeguard themselves in cyberspace against cyber threats and attacks. They will further be expected to utilize the information and messages available on the safe use of the cyberspace.

4.2 Funding and Resources

The successful implementation of Malawi's NCS is fully dependent on adequate funds and resources. Considering that ICTs and Cyberspace spur socio-economic growth, the National Cybersecurity Strategy implementation logical frameworks have identified possible lead organization and funding sources for various measures proposed in the NCS.

4.3 Monitoring and Evaluation

The implementation of the NCS will require a Monitoring and Evaluation Framework that:

- supports the attainment of the NCS Vision and Strategic Goals; and

- enables accurate reporting on progress and identification of lessons learned and challenges encountered for informed decision making and effective planning.

This can be used to elaborate new measures as well as amend and tailor existing initiatives under the strategy. This section of the Strategy details the proposed systematic approach to monitoring and evaluating progress as an integral part in implementing the NCS of Malawi. The monitoring is scheduled to be periodic in order to track the progress of implementation of the NCS. The monitoring will, therefore, focus on periodic and objective assessment of progress towards the attainment of the set objectives.

The key objectives of the monitoring and evaluation approach are:

- Establishment of Performance Targets for various governmental institutions or relevant stakeholders responsible for implementing specific actions of the NCS.

- Development of performance plans to establish a shared understanding of the expected end results, the approach to achieving these end results and identify the resources necessary to ensure a successful implementation. The plans will be based on the KPIs, Performance Targets and Deadlines provided in the Implementation Logical Framework

- Monitoring and reporting performance and progress in achieving expected end results by identifying and promptly reporting observed or likely deviations.

- Periodically evaluating institutional or individual performance against established performance targets

- An independent stakeholder will be commissioned to undertake the mid-term and long-term review of the strategy to determine the long-term impact and outcomes of the strategy based on periodic reviews, and if necessary effect remedial actions to keep implementation on track. The mid-term review will be undertaken at the end of 3rd Quarter of Year 3 of the Strategy and the long term review at the end of the 4th year.

MACRA and all relevant Stakeholders will develop a comprehensive Monitoring and Evaluation Plan which will be based on the proposed approach within 3 months of the adoption of the Strategy. The Monitoring and Evaluation Plan will enable the assessment of the operational issues encountered during the implementation of the strategy, as well as the assessment of the

long-term impact and outcomes of the strategy based on periodic reviews. The Monitoring and Evaluation Plan will also provide mechanisms or tools for data collection and reporting, and further information on the roles and responsibilities of stakeholders, and frequency of reports.

APPENDIX A - NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION LOGICAL FRAMEWORKS

This section presents the key elements necessary to successfully implement the strategy detailed in Chapter 3 and these include:

- Strategic Goal: the substantive long term goal that Malawi would like to achieve in each priority area;

- Specific Objective: the specific steps to be undertaken to achieve the Strategic Goal

- Strategies/Actions: The activities that must be undertaken, under this Strategic Plan, in pursuit of the Specific Objective objectives

- Deliverables/Outputs: The formal work products that Malawi will achieve in the pursuit of the objectives and the implementation of the Strategy

- Lead Implementing Agency and Support: The Malawian Institutions with primary responsibility for managing completion of each objective, and the institutions that will provide support.

- Time Period: Period of time within which deliverables/outputs are produced and/or Strategies/Actions are implemented.

- Key Performance Indicators: The indices, data measurements, and trends that should be monitored to evaluate the progress in implementing the Strategy and achieving the objectives and deliverables

- Possible Funding Sources and Mechanisms: An overview of different possible funding sources and mechanisms that can be adopted by Malawi to fund the implementation of the NCS

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
Strategic Goal – 1: Identify and manage the Critical Information Infrastructure of Malawi						
3.4.1 Specific Objective 1: **Identify and protect the Critical Information Infrastructure of Malawi**	3.4.1.1 Establish a national CII register	National CII Register	MACRA/Malawi CERT/Ministry of ICT	Within 6 months and continuous	Publication of National CII Register	MACRA/Malawi CERT
	3.4.1.2 Develop a National CII Governance Framework which provides details on CII protection procedures and processes	National CII Governance Framework	MACRA/Malawi CERT Malawi CII/ Ministry of ICT	Within 6 months and continuous	Publication of National CII Governance Framework which provides details on CII protection procedures and processes	MACRA/Malawi CERT
	3.4.1.3 Establish a National Risk Register and regulations and/or guidelines that promote continuous risk assessment and management across CIIs in Malawi	Risk assessment and management guidelines for CIIs National Risk Register	MACRA/Malawi CERT Malawi CII/ Ministry of ICT	Within 6 months and continuous	Frequency of Risk assessment exercises Frequency of update to National Risk Register	MACRA/Malawi CERT Malawi CII
	3.4.1.4 Establish mandatory equipment specifications, Mandatory guidelines, regulations, security requirements, procedures relating to the management of risks by CIIS	CII Minimum security standards and procedures including security audits, equipment specifications, SOPS, Access	Ministry of ICT MACRA/MALAWI CERT	Within 12 months and continuous	Extent of implementation of standards, procedures, guidelines, ,specifications, Equipment Specifications, SOPS, Access	Ministry of ICT MACRA/MALAWI CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		Control Mechanisms, etc.			Control Mechanisms, etc.	
	3.4.1.5 Create a National Vulnerability Register and Framework for regular vulnerability monitoring and disclosure for CII	National Vulnerability Register and Vulnerability Disclosure Framework	MACRA/MALAWI CERT CII /Ministry of ICT	Within 6 months and continuous	Frequency of update of vulnerability register Frequency of vulnerability disclosures	MACRA/Malawi CERT CII
	3.4.1.6 Undertake continuous monitoring and regular testing to detect errors, vulnerabilities, and intrusions in CII	Security Audits and tests to detect errors and vulnerabilities Intrusion detection systems/exercises	CII Ministry of ICT MACRA/Malawi CERT	Within 6 months and continuous	Number and frequency of security audits and tests; Effectiveness of security audits and tests Effectiveness of intrusion detection tests/systems;	CII
	3.4.1.7 Promote and enhance regional and international cooperation in the protection of the critical information infrastructure (CII)	Regional and international collaboration programmes Enhanced	Ministry of ICT MACRA/MALAWI CERT	Within 6 months and continuous	Extent of international cooperation in the protection of CII	Ministry of ICT MACRA/MALAWI CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		collaboration and information sharing mechanism MOUs with international partners on the monitoring, analysis and management of cross border CII				
3.4.2 Specific Objective 2: **Continuously monitor and manage cyber threats and risks to enhance incident response**	3.4.2.1 Expedite the establishment and operationalization of a national CERT with clear processes, defined roles and responsibilities	Establish and operationalize CERT hosted at MACRA	MACRA/Malawi CERT Ministry of ICT	Within 6 months and continuous	Extent of operationalization of MACRA/Malawi CERT Effectiveness of MACRA/Malawi CERT	MACRA/Malawi CERT
	3.4.2.2 Continuously develop the capacity of staff at Malawi CERT to address the fast changing technical requirements, and develop abilities to actively obtain information in cyberspace, about current cyber risks and threats	Malawi CERT Training Programme	MACRA/Malawi CERT	Within 12 months of strategy adoption	Number and frequency of MACRA/Malawi CERT Training sessions; Number of incidents/attacks/threats/risks	MACRA/Malawi CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
					prevented/mitigated by forensic detection and analysis	
	3.4.2.3 Develop a national incident reporting, information sharing and coordination mechanisms to address reporting of incidents and coordination in incident response	National Incident Reporting and Information Sharing Framework	MACRA/Malawi CERT	Within 6 months and continuous	Effectiveness and adaptability of the incident reporting and information sharing awareness raising Framework	MACRA/Malawi CERT
	3.4.2.4 Create and continuously update cyber security incidents register, assess incidents, and suggest measures to resolve issues and mitigate threats and risks	Real time cyber security incident registers; Measures to mitigate threats, risks and resolve incidents	MACRA/Malawi CERT	Within 6 months and continuous	Extent of updates of incident registers; Extent of implementation of mitigation measures	MACRA/Malawi CERT
	3.4.2.5 Specify minimum and mandatory log/register requirements necessary for dependable cyber security incident analysis	Minimum and mandatory log requirements	MACRA/Malawi CERT	Within 6 months and continuous	Level of awareness of Minimum and mandatory log requirements	MACRA/Malawi CERT
	3.4.2.6 Continuously monitor, analyze and assess Cyber threats and potential risks and be able to provide a real time	Real time overview of the state of cybersecurity	MACRA/Malawi CERT	Within 6 months and continuous	Frequency of updates to overview of the state of cybersecurity	MACRA/Malawi CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	overview of the state of cybersecurity across nation					
	3.4.2.7 Develop a Cybersecurity Governance Framework for defining roles and responsibilities of all stakeholders in the cybersecurity ecosystem as well as describe SOPs and code of conduct in responding to incidents	Cybersecurity Governance Framework that roles and responsibilities of all stakeholders in the cybersecurity ecosystem as well as describe SOPs and code of conduct in responding to incidents	Ministry of ICT MACRA/Malawi CERT	Within 6 months and continuous	Extent of effectiveness in responding to incidents nationwide	MACRA/Malawi CERT
	3.4.2.8 Establish a call center/help line for reporting incidents or seeking assistance with incidents	National Cyber Security Call Center/Help Line	MACRA/Malawi CERT	Within 6 months and continuous	Number of calls to help line or call center Extent of incidents addressed through call line	MACRA/Malawi CERT
	3.4.2.9 Develop and implement cybersecurity incident simulation scenarios and programs that can be used during the national exercises	Cybersecurity incident simulation scenarios and programs	MACRA/Malawi CERT	Within 6 months and continuous	Usage of cybersecurity incident simulation scenarios and programs during national exercises	MACRA/Malawi CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	3.4.2.10 Develop and continuously update cybersecurity contingency plans, which will include roles of the military/security forces role during cyber-attacks and emergencies	Sector specific contingency plans (reviewed annually)	MACRA/Malawi CERT Malawi Defence Force	Within 6 months and continuous	Level of awareness of Sector specific contingency plans	MACRA/Malawi CERT Malawi Defence Force
	3.4.2.11 Develop and test requisite crisis management measures during frequent cyber drills	National crisis management Measures for Malawi Frequent cyber drills	MACRA/Malawi CERT	Within 6 months and continuous	Level of awareness of National crisis Management measures for Malawi	MACRA/Malawi CERT
	3.4.2.12 Evaluate cyber drills to develop options on how to improve crisis management measures	Lessons/Results of cyber drill exercise Frequent cyber drills	Malawi CERT MDF	Within 12 months and continuous	Frequency of cyber drill exercises No. of revisions of contingency plans	Malawi CERT MDF
	3.4.2.13 Develop a Cyber Defence Strategy that details approaches to addressing threats to national security in	National Cyber Defence Strategy	MDF	12 months	Extent of implementation of Cyber Defence Strategy	MDF

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	cyberspace					
	3.4.2.14 Establish a Central Defence Command and Control Centre for cybersecurity in Malawi	A Central Defence Command and Control Centre for cybersecurity	MDF	12 months	Extent of operationalization of a Central Defence Command and Control Centre for cybersecurity	MDF
Strategic Goal – 2: Develop and enhance cybersecurity-related capacity, infrastructure, legal, regulatory and other related frameworks						
3.4.3 Specific Objective 3: **Strengthen Malawi's legal and regulatory frameworks to enhance cybersecurity in Malawi**	3.4.3.1 Undertake a gap analysis to identify gaps in current ICT Security legal and regulatory framework and develop requisite instruments to address Gaps including issues relating to privacy and data protection.	A gap analysis to identify gaps in current ICT security legal and regulatory framework Requisite instruments to address Gaps including issues relating to privacy and data protection	Ministry of ICT Ministry of Justice and Constitutional Affairs MACRA	1 year	Enacted amendments to existing legislations or policies Enactment of new policies/legislations	Ministry of ICT Ministry of Justice and Constitutional Afairs MACRA
	3.4.3.2 Develop and publish a cybersecurity policy and standards consisting of general and sector-specific cybersecurity controls that would be recognized as a	A Cybersecurity Framework (CSF) consisting of general and sector-specific policies and controls	Ministry of ICT MACRA	Within 6 months and continuous	Extent of adoption/implementation of A Cybersecurity Framework (CSF)	Ministry of ICT MACRA

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	national standard					
	3.4.3.3 Create a national programme to promote the adaptation and adoption of cyber standards across government institutions and CII in Malawi	Deployment of national cyber standards across the nation	Ministry of ICT MACRA Malawi Bureau of Standards	Within 6 months and continuous	Extent of adoption/implementation of cyber standards across the nation	Ministry of ICT MACRA Malawi Bureau of Standards
3.4.4 Specific Objective 4: **Stakeholder capacity building for law enforcement and judiciary to implement cybersecurity related laws**	3.4.4.1 Identify needs and then provide training and education to develop the capacities of the law enforcement agencies, judiciary and the legal fraternity on how to interpret and enforce the policy, legal & regulatory frameworks on cybersecurity in Malawi	Training programme for law enforcement agencies and judiciary on how to interpret and enforce the policy, legal & regulatory frameworks on cybersecurity in Malawi Strong law enforcement and judiciary capable enforcing the	Law Enforcement and Judiciary	Within 6 months and continuous	Number of capacity building programmes conducted Capacity of Law Enforcement and Judiciary in enforcing the policy, legal & regulatory frameworks on cybersecurity in Malawi	Law Enforcement and Judiciary

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		policy, legal & regulatory frameworks on cybersecurity in Malawi				
3.4.5 Specific Objective 5: **Enhance technical and procedural measures for implementing cybersecurity for CIIs**	3.4.5.1 Establish mandatory and minimum technology and security requirements for equipment of ISPs and end users like the banking sector	Mandatory and minimum technology and security requirements for equipment of ISPs and end users	MACRA/Malawi CERT CIIs, ISPs and other end users	Within 6 months of adoption of strategy and continuous	Extent of identification of equipment that don't meet the minimum technology or security requirements	MACRA/Malawi CERT CIIs, ISPs and other end users
	3.4.5.2 Develop a national government programme to deploy and manage government ICT infrastructure	National programme to deploy and manage government ICT infrastructure	Ministry of ICT	Within 12 months of adoption of NCS and continuously reviewed	Extent of implementation of national programme to deploy and manage government ICT infrastructure	Ministry of ICT
	3.4.5.3 Develop a national programme to enhance internet infrastructure development and resilience.	national programme to enhance internet infrastructure development and resilience	Ministry of ICT	Within 12 months of adoption of NCS and continuously reviewed	Extent of implementation of national programme to national programme to enhance internet infrastructure development and	Ministry of ICT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
					resilience	
	3.4.5.4 Develop National Contingency plans which identify emergency response asset priorities and standard operating procedures (SOPs)	National contingency plan	MACRA/Malawi CERT Malawi Defence Force	Within 12 months of adoption of NCS and continuously reviewed	Adoption of national contingency plan including the emergency response asset priorities and standard operating procedures (SOPs)	MACRA/Malawi CERT Malawi Defence Force
	3.4.5.5 Review and update the map of current emergency response assets	Emergency response asset map	MACRA/Malawi CERT Malawi Defence Forces	Within 12 months of adoption of NCS and continuously reviewed	Completion of emergency response asset map	MACRA/Malawi CERT Malawi Defence Forces
	3.4.5.6 Ensure communication channels are deployed across emergency response functions, geographic areas of responsibility, public and private responders, and command authority	Emergency Communication Network	ICT/Communications service providers Malawi Defence Forces	Within 12 months of adoption of NCS and continuously reviewed	Extent of deployment of Emergency Communication Network	ICT/Communications Service Providers Malawi Defence Forces
3.4.6 Specific Objective 6: **Continuously develop and enhance the**	3.4.6.1 Revise the National Research Agenda to promote R&D in cybersecurity across Malawi	Revised National Research Agenda which includes the cybersecurity aspects	Ministry of Education, Science and Technology (MoEST)	Within 12 months of adoption of NCS and continuously reviewed	Extent of implementation of Revised National Research Agenda which includes the cybersecurity	Ministry of Education, Science and Technology (MoEST)

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
cybersecurity technical capacity in Malawi			Academia Ministry of ICT National Commission for Science and Technology (NCST)		aspects	Academia Ministry of ICT National Research Council
	3.4.6.2 Establish a National Centre of Excellence for cybersecurity training & research	Operational National Centre of Excellence for cybersecurity training & research	Ministry of ICT Ministry of Education, Science and Technology (MoEST) Academia National Commission for Science and Technology (NCST)	Within 12 months of Strategy Adoption	Extent of operationalization of National Centre of Excellence	Ministry of Education, Science and Technology (MoEST) Academia Private sector
	3.4.6.3 Review and update primary, secondary and tertiary level education curriculum to include cybersecurity elements	Revised education curriculum which includes aspects about	Ministry of Education, Science and Technology (MoEST)	Within 12 months of Strategy Adoption	Extent of implementation of revised curriculum	Ministry of Education, Science and Technology (MoEST)

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		cybersecurity	Academia			
	3.4.6.4 Support cybersecurity competitions and R & D projects in universities and schools	Funding and incentive programmes for universities engaged in cybersecurity R & D competitions in schools on cybersecurity	Academia; Ministry of Education, Science and Technology (MoEST) Private sector National Commission for Science and Technology (NCST)	Within 12 months of strategy adoption and continuously after	Number of universities participating in funding and incentive programme	Academia; Ministry of Education, Science and Technology (MoEST) Private sector
	3.4.6.5 Support national enterprises providing cybersecurity solutions, and undertaking R & D in cybersecurity	Funding and incentive programmes for Enterprises engaged in cybersecurity R & D	Academia; Ministry of Education, Science and Technology (MoEST)	Within 12 months of strategy adoption and continuously after	Number of Enterprises participating in funding and incentive programme	Special incentive programmes provided by Ministry of finance
	3.4.6.6 Collaborate with universities, colleges and the private sector to create new study and internship programs on cyber security	New tertiary level study and internship programs on cybersecurity	Academia Ministry of Education, Science and	Within 12 months of strategy adoption and continuously	Number of new tertiary level study and internship programs on Cyber security created;	Academia Ministry of Education, Science and

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
			Technology (MoEST) Ministry of Labour, Youth, Sports and Manpower development Private Sector	after	Number of students/graduates enrolled at new tertiary level study and internship programs on cyber security created	Technology (MoEST) Ministry of Labour Private Sector
	3.4.6.7 Collaborate with the private sector and academia to support participation of government institutions, universities, private sector in regional and international research projects and exercises relating to cybersecurity	Partnerships to support participation of government institutions, universities, private sector in regional and international research projects and exercises relating to cybersecurity	Academia Ministry of Education, Science and Technology (MoEST) National Commission for Science and Technology (NCST)	Within 12 months of strategy adoption and continuously after	Extent of participation in national and international research projects and activities concerning cyber security; Number of partnerships created which support participation in national and international research projects and activities concerning cyber security;	Academia Ministry of Education, Science and Technology (MoEST) Ministry of Labour National Commission for Science and Technology

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	3.4.6.8 Create standards in cybersecurity training and education	Standards for cybersecurity training and education	Ministry of Education, Science and Technology (MoEST)	Within 12 months of strategy adoption and continuously after	Certifiable Levels of competence of the trained individuals	Academia Ministry of Education, Science and Technology (MoEST)
	3.4.6.9 Train IT personnel of various Government ministries and institutions on how to detect incidents, report incidents, and collaborate with the Malawi CERT and institutions from other sectors on cybersecurity	Training programme for IT personnel of various Government ministries and institutions	OPC/Department of Human Resources Management and Development(DHRMD) Academia Ministry of Education, Science and Technology (MoEST) Ministry of Labour Ministry of ICT	Within 12 months of strategy adoption	Number and frequency of courses/ qualifications delivered / acquired	OPC/Department of Human Resources Management and Development(DHRMD) Ministry of Education, Science and Technology (MoEST) Ministry of Labour Ministry of ICT
3.4.7 Specific Objective 7:	3.4.7.1 Develop National and Career Progression Policy promoting	National Policy promoting continuous	OPC/Department of Human Resources	6 months and continuously after	Extent of implementation of Career progression	OPC/Department of Human Resources

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
Facilitate the recruitment of, and retention of cybersecurity expertise within Malawi	continuous training and education for Incident response and addressing issues relating to cybersecurity	training and education for incident response and addressing countermeasures for CERT and security personnel Career progression strategy that promotes continuous professional education	Management and Development(DHRMD) Ministry of Labour		strategy Extent of national policy promoting continuous training and education	Management and Development(DRHRD) Ministry of Labour
	3.4.7.2 Identify the staffing requirements for Government agencies and Critical Infrastructure operators and develop a national recruitment and retention strategy	Set of staffing requirements for Government agencies and Critical Infrastructure operators Cybersecurity staffing recruitment and retention strategy	OPC/Department of Human Resources Management and Development(DHRMD) Ministry of Labour	1 year	Extent of cybersecurity staffing recruitment and retention	OPC/Department of Human Resources Management and Development(DHRMD) Ministry of Labour
	3.4.7.3 Develop and	National	OPC/Departmen	Within 6	Number and	OPC/Department

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	implement cybersecurity training and capacity building training plans for Government personnel	cybersecurity training and capacity building training plans for Government Personnel	t of Human Resources Management and Development(DHRMD) Ministry of Labour	months and continuous	frequency of courses/ qualifications delivered / acquired	of Human Resources Management and Development(DHRMD) Ministry of Labour
Strategic Goal – 3: Promote awareness, information sharing and collaboration on cyber security						
3.4.8 Specific Objective 8: **Enhance cyber security awareness across the general public and national institutions**	3.4.8.1 Undertake a nationwide assessment to determine level of awareness of cybersecurity across the nation	Assessment of national levels of cybersecurity awareness	MACRA/Malawi CERT	Within 6 months of adoption of strategy and continuously after	Extent of assessment of national levels of cybersecurity awareness	MACRA/Malawi CERT
	3.4.8.2 Develop and implement a national roadmap for improving awareness of current cyber security trends and threats	National roadmap for improving awareness of current cyber security trends Up to date and functional website with	MINISTRY of ICT MACRA/Malawi CERT	Within 6 months and continuous	Level of awareness Number/frequency of cybersecurity campaigns Effectiveness of campaigns Number of	MINISTRY of ICT MACRA/Malawi CERT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		information current cyber security threats, risks, vulnerabilities, etc.; Awareness campaigns to raise awareness of cybersecurity trends and threats			revisions to website	
	3.4.8.3 Develop and disseminate national cybersecurity Best practices to engrain a cybersecurity mindset in the public	National cybersecurity best practices	MACRA/Malawi CERT	Within 6 months of adoption of strategy and continuously after	Extent of dissemination of cybersecurity Best practices	MACRA/Malawi CERT
	3.4.8.4 Undertake mandatory training of Board Members of different organizations to enhance their understanding of cyber issues and how their organizations address these threats	Mandatory training of Board Members of different organizations	MACRA CII	Within 6 months of adoption of strategy	Extent of Board member's knowledge of cybersecurity and how their organizations address	MACRA CII
3.4.9 Specific Objective 9: **Promote**	3.4.9.1 Create a national forum to enhance and promote information sharing and collaboration	National Forum for national information sharing and	MACRA, Ministry of ICT	Within 6 months of adoption of strategy and	Level of national participation at national forum	MACRA, Ministry of ICT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
collaboration and information sharing on Cybersecurity	nationally on cybersecurity	collaboration		continuously after		
	3.4.9.2 Continuously update the citizens, the private sector and the public sector, on information related to cyber threats, vulnerabilities, incidents, activities across the nation to foster trust	Online Platform which provides national cybersecurity-related information	MACRA, Ministry of ICT	Within 6 months of adoption of strategy and continuously after	Frequency of updates of online platform	MACRA, Ministry of ICT
Strategic Goal – 4: Enable and continuously improve the safety of vulnerable groups in cyberspace, especially the safety of children						
3.4.10 Specific Objective 10: **Ensure online safety for vulnerable groups, especially children**	3.4.10.1 Develop and disseminate online safety guidelines and best practices to protect vulnerable groups in Malawi, especially children, from cyber threats	Guidelines and best practices to protect children and other vulnerable groups from cyber threats	MACRA, Ministry of ICT, CONGOMA	Within 6 months and continuously after	Frequency of publication, review and update of best practices and guidelines Frequency of dissemination of best practices and guidelines	MACRA, Ministry of ICT, CONGOMA
	3.4.10.2 Deploy special awareness programmes to	Special online Safety	MACRA, Ministry of ICT,	Within 6 months and	Extent of implementation of	MACRA, Ministry of ICT,

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	target and inform children and other vulnerable groups about safe and responsible use of the internet	awareness programme for children and other vulnerable groups	CONGOMA	continuously after	special online safety awareness programme for children and other vulnerable groups Number of children and members of other vulnerable groups with skills on how to use the internet safely	CONGOMA
3.4.11 Specific Objective 11: **Deploy tools to keep vulnerable groups, especially children are safe online**	3.4.11.1 Promote the deployment of technical measures or web filtering tools that prevent access to harmful content by children and other vulnerable groups	Wide deployment of technical measures to prevent access to harmful content by children and other vulnerable groups	Operators; ISPs	Within 3 months of adoption of national strategy and continuously after	Extent of deployment of technical controls or measures like parental control or authentication services Extent of usage of technical controls or measures like parental control or authentication services	Operators; ISPs
	3.4.11.2 Encourage ISPs and other services providers to make their clients, especially parents and guardians aware of how to leverage available	Knowledge and awareness of tools/technologies that can be deployed by ISPs and other	MACRA Operators; ISPs	Within 6 months of adoption of national strategy and continuously	Extent of dissemination of information on tools/technologies that can be deployed by ISPs	MACRA Operators; ISPs

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	tools/technologies to manage potential risks to vulnerable groups while accessing services online	service providers to keep children and other vulnerable groups safe online;		after	and other service providers Extent of usage of technical controls or measures like parental control or authentication services	
Strategic Goal – 5: Enhance and coordinate the fight against all forms of cybercrime						
3.4.12 Specific Objective 12: **Enhance Cybercrime detection**	3.4.12.1 Establish the requisite framework to establish and operationalize a digital forensics laboratory	Operational digital forensics laboratory Plans and budgets to establish Digital forensics lab	Malawi Police Services Ministry of Justice and Constitutional Affairs	Within 24 months of strategy adoption	Extent of operationalization of Digital Forensics Lab	Malawi Police Services Ministry of Justice and Constitutional Affairs

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	3.4.12.2 Develop mandatory digital forensics and evidence handling courses for the judiciary, law enforcement and personnel from other related agencies involved in the detection and prosecution of cybercrime	Training programme on digital forensics and evidence handling	Malawi Police Services, Ministry of Justice and Constitutional Affairs	Continuously starting 12 months of strategy adoption	Number and frequency of mandatory courses and qualifications delivered to or acquired on cybercrime by judiciary and security personnel nationwide No of successful prosecutions of cybercrimes	Malawi Police Services Ministry of Justice and Constitutional Affairs
	3.4.12.3 Build and enhance capacity to detect cybercrime incidents	Training Programme and Budget on cybercrime incident detection	Malawi Police Services, Ministry of Justice and Constitutional Affairs.	Continuously starting 12 months of strategy adoption	Number and frequency of mandatory courses and qualifications delivered to or acquired on cybercrime by judiciary and security personnel nationwide Extent of detection of cybercrimes	Malawi Police Services Ministry of Justice and Constitutional Affairs.

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
3.4.13 Specific Objective 13: **Enhance cooperation and awareness in the fight against cybercrime**	3.4.13.1 Develop and continuously update an information sharing, governance and collaboration framework for the fight against cybercrime which will include links that ensure direct and timely collaboration between judiciary, law enforcement and personnel from other related agencies, service providers, CII entities, MACRA/Malawi CERT and other government institutions on issues that concern cybercrime and cybersecurity	Governance Framework for fight against cybercrime	Malawi Police Forces Other Security Forces; Judiciary and Ministry of Justice and Constitutional Affairs. MACRA/MALAWI CERT	Continuously starting 12 months of strategy adoption	Extent of collaboration across all relevant stakeholders in the fight against cybercrime and ensuring Cybersecurity	Malawi Police Forces Other Security Forces; Judiciary and Ministry of Justice and Constitutional Affairs. MACRA/MALAWI CERT
3.4.14 Specific Objective 14: **Promote international collaboration in the fight against cybercrime**	3.4.14.1 Strengthen collaboration with regional, international states and partners in combating cybercrime through treaties, conventions (e.g. Budapest) and bilateral agreements, especially through frameworks such as the 24/7 cybercrime Network, mutual legal assistance frameworks, etc.	Signatures of relevant international treaty agreements on cybercrime MOUs between other countries and international partners Participation in	Ministry of Foreign Affairs and International Cooperation Malawi Police Service	Continuously starting within 6 months of adoption of national strategy	No of signed MOUs No of signed international treaties Extent of participation at international fora on cybercrime	Ministry of Foreign Affairs Malawi Police Forces

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
		international forums on cybercrime				
	3.4.14.2 Develop a clear plan that outlines how to manage international collaboration across multiple strategy areas such as law enforcement, incidence response, research and innovation in cybersecurity.	International collaboration management plan Improved international collaboration	MACRA, Ministry of ICT	Within 6 months of adoption of strategy and continuously after	Effectiveness and efficiency in international collaboration Extent of collaboration and information sharing internationally	MACRA, Ministry of ICT
	3.4.14.3 Subscribe to and participate in all relevant regional and international forums on cybersecurity.	Improved regional and international collaboration on cybersecurity Participation in relevant regional and international fora on cybersecurity	MACRA, Ministry of ICT	Within 6 months of adoption of strategy and continuously after	Effectiveness and efficiency in international collaboration Extent of participation in regional and international for a on cybersecurity	MACRA, Ministry of ICT
Strategic Goal – 6: Promote use of secure cyberspace to drive social and economic development						
3.4.15 Specific Objective 15:	3.4.15.1 Undertake the transition	IPV4 to IPV6 Implementation Plan	Ministry of ICT Ministry of ICT	Within 18 months of strategy	Extent of implementation of IPV4 to IPV6	Ministry of ICT Ministry of ICT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
Cooperate with the private sector to ensure that cyberspace, reliably and securely, supports information sharing, R&D, and entrepreneurship	from IPV4 to IPV6 protocol and disseminate information on the benefits of the transition, especially IPV6 security features relating to confidentiality, authentication and data integrity			adoption	Transition	
3.4.16 Specific Objective 16: **Foster trust and confidence in cyberspace, especially in applications relating to e-government and e-commerce**	3.4.16.1 Create, and continuously update the general public and public sector on how cyberspace is securely used in Malawi to deliver e-government and e-commerce services in Malawi, highlighting the various security features deployed to foster trust	E-Governance and E-commerce services awareness campaign that highlights the security features of	Ministry of ICT	Continuously starting within 6 months of adoption of strategy	Extent of awareness of E-Governance and E-Commerce services and security features	Ministry of ICT
	3.4.16.2 Encourage the use of Public Key Infrastructure (PKI) for transactions to/from Government Ministries, Departments and Agencies to enhance high cybersecurity levels and trust in delivering	PKI implementation plan	Ministry of ICT	Within 12 months of strategy adoption	No. of Government ICT systems and applications incorporating usage of PKI	Ministry of ICT

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
	public services.					
	3.4.16.3 Appoint cybersecurity inspectors who among other duties, will serve as Focal Points of contact to support small and medium enterprises in addressing Cybersecurity needs and methods of mitigating cyber threats.	Cybersecurity inspectors to support small and medium enterprises on cybersecurity	MACRA	Within 6 months of strategy adoption	Extent of support provided to SMEs	MACRA