The United Republic of Tanzania

Ministry of Works, Transport and Communication
(Communication Sector)

National Cyber Security Strategy
2018 –2023

April, 2018

FOREWORD

The Government of the United Republic of Tanzania is an East Africa Countries hub of exchange and commerce. Tanzania policies has recognized that we must always be open to new technologies and know-how, in order to connect ideas, economies and cultures for social economic development.

Digitally, Tanzania is one of the most connected nations in the East Africa. We connected to the world through three main optic fibres landing in Dar Es Salaam on the Indian Ocean. We also have a national backbone optic fibre broadband network linking to the 9 points with neighboring countries. We have long embraced information and communication technologies for economic and social development. Today, we have more mobile phone numbers than adult people. The mobile internet access is almost 46% penetration of the 42 million mobile phone users.

However, reliance on information communication technologies also makes us vulnerable. Cyber threats and attacks are becoming more sophisticated, with more severe consequences. We cannot take cybersecurity for granted. The Cybersecurity Strategy outlines Tanzania's vision, goals and priorities. We are determined to protect essential services from cyber threats, and to create a secure cyberspace for businesses and communities. The Government Cyber Security and Computer Emergency Response Team (CERT) and cyber crime unit under the Tanzania Police Force will take the lead, and work with other agencies and private sector partners to achieve this.

The Government cannot do it alone. Businesses are responsible for protecting customers' personal data. Individuals need to practice good cyber security to keep personal devices and data safe. If we each do our part to use our systems and devices responsibly, then collectively we can help to protect Tanzania's cyberspace.

Cyber attackers do not respect jurisdictions. All countries, especially highly-connected ones due to geographical position including Tanzania, benefit from international cooperation in securing global information communication infrastructures and responding to cyber threats. Tanzania will work closely with other countries to build consensus in cyber norms, strengthen capacity and address cyber threats and crimes.

As an industry, cybersecurity offers opportunities and good jobs for Tanzanians. The Government will provide education and training opportunities for those who wish to pursue a career in cybersecurity. Together, we will build a resilient and trusted cyber environment that harnesses the benefits of technology to improve the social economic welfare of our Citizens.

Sasabo .

Mrs. Maria Sasabo (PhD)

PERMANENT SECTRETARY COMMUNICATIONS

ACKNOWLEDGEMENT iv

LIST OF ACRONYMS v

EXECUTIVE SUMMARY viii

CHAPTER ONE 1

1. INTRODUCTION 1

1.1. Background 1

1.2. Scope 2

1.3. Strategy Development Approach 2

1.4. The Layout and Structure of the Strategy 2

CHAPTER TWO 3

2. SITUATION ANALYSIS 3

2.1 Policy and Strategy 3

2.1.1 Official National Cyber Security Strategy 3

2.1.2 Incident Response 3

2.1.3 National Critical Information Infrastructure (CII) Protection 4

2.1.4 Crisis Management 4

2.2 Culture and society 5

2.2.1 Cyber Security mindset 5

2.2.2 Cyber Security Awareness 5

2.2.3 Confidence and trust in online services 6

2.2.4 Privacy online 6

2.3 Cyber Security Education, Skills and Training 7

2.3.1 Availability of Cyber Security education 7

2.3.2 National Development of Cyber Security Education 7

2.3.3 Corporate Governance, Knowledge and Standards 8

2.4 Legal and Regulatory Frameworks 8
2.4.1 Cyber Security Legal Frameworks 8
2.4.2 Legal Investigation and Prosecution 8
2.4.3 Vulnerability Reporting 9
2.5 Standards, Organizations and Technologies 9
2.5.1 Adherence to Standards 9
2.5.2 National Infrastructure Resilience 10
2.5.3 Online Marketplace 10
2.6 Table1: SWOC Analysis 11
2.7 Critical Issues 15
CHAPTER THREE 17
3. THE STRATEGY PLAN 17
3.1 Vision 17
3.2 Mission 17
3.3 Guiding Principles 17
3.3.1 Principle 1 - Multistakeholder Partnerships 17
3.3.2 Principle 2 - Ubiquitous threats 17
3.3.3 Principle 3 - Risk based Management 17
3.3.4 Principle 4 – Capacity building and Awareness for All 18
3.3.5 Principle 5 - Regional and International collaboration 18
3.4 Strategic Goals 18
Goal 1: Ensure protection of critical information infrastructure 18
Goal 2: Increase Cyber Security technical capabilities and awareness across Tanzania 20
Goal 3: Promote local, regional and international collaboration in Cyber Security 22
Goal 4: Enhance the national response to Cyber Security threats/trends 24

Goal 5: Enhance legal and regulatory frameworks to support Cyber Security initiatives in Tanzania 25

3.5 Governance Structure, Key Stakeholders and Resources for Implementing the Strategy 26

4. Key Stakeholders 27

5. Proposed Governance Structure 29

6. Resources for Implementing the Strategic Plan 30

7. ANNEX 1: Matrix of the implementation of the National Cyber Security Strategy (NCSS) 31

ACKNOWLEDGEMENT

The National Cyber Security Strategy (NCSS) is a collaborative endeavor involving experts from the Ministry of Works, Transport and Communication (MWTC), Tanzania Communications Regulatory Authority (TCRA), the Commonwealth Telecommunication Organization (CTO), relevant Ministries, Departments and Agencies; and Local Government Authority (LGAs) from across the Government of the United Republic of Tanzania and private sector representatives. Special thank is owed to the chairmen, secretaries and members of the National Working groups. The Government of the URT through MWTC would like to acknowledge and thank all contributors for their hard work and commitment to completing this strategy, and more importantly, to fulfilling the mission and realizing the vision of the NCSS.

LIST OF ACRONYMS

Acronym	**Description**
AGC	Attorney General's Chambers
ATM	Automated Teller Machine
AU	African Union
BCP	Business Continuity Plans
BOT	Bank of Tanzania
BRT	Bus Rapid Transit
CEIR	Central Equipment Identification Register
CII	Critical Information Infrastructure
CMM	Cyber Security Capacity Maturity Model
COSTECH	Tanzania Commission for Science and Technology
CTO	Commonwealth Telecommunications Organization
DAWASA	Dar es Salaam Water and Sewerage Authority
DPP	Director of Public Prosecution
DRAM	Department of Records and Nation Archives
DRP	Disaster Recovery Plan
EAC	East African Community
EASSy	Eastern Africa Submarine Cable System
eGA	e- Government Agency
EPOCA	Electronic and Postal Communication Act
EU	European Union
FCC	Fair Competition Commission
HESLB	Higher Education Students' Loans Board
ICT	Information and Communication Technology
ICTC	Information and Communication Technology Commission
IP/MPLS	Internet protocol/ Multi-Protocol Label Switching
IP-SEC	Internet Protocol Security
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
ISP	Internet Service Provider
ITU	International Telecommunications Union
IXP	Internet Exchange Point
LGAs	Local Government Authorities
LRC	Law Reform Commission
MDAs	Ministries, Departments and Agencies
MNO	Mobile Network Operators
MOAT	Media Owners Association of Tanzania
MoDNS	Ministry of Defence and National Service
MOEST	Ministry of Education, Science and Technology

Acronym	**Description**
MoFAEARIC	Ministry of Foreign Affairs, East Africa, Regional and International Cooperation
MoFP	Ministry of Finance and Planning
MoHA	Ministry of Home Affairs
MoHCDGSC	Ministry of Health, Community Development, Gender, Senior and Child
MoICAS	Ministry of Information, Culture, Arts and Sports
MoITI	Ministry of Industry, Trade and Investment
MoJCA	Ministry of Justice and Constitutional Affairs
MoLE	Ministry of Labour and Employment
MoU	Memorandum of Understanding
MWTC	Ministry of Works, Transport and Communication
NAO	National Audit Office
NCRC	National Cyber Security R&D Centre
NCSS	National Cyber Security Strategy
NECTA	The National Examinations Council of Tanzania
NICTP	National ICT Policy
NICTBB	National ICT Broadband Backbone
NIDA	National Identification Authority
NMB	National Microfinance Bank
NPKI	National Public Key Infrastructure
NSOC	National Security Operation Center
PMO	Prime Minister's Office
PO	President's Office
PO-PSM	President's Office – Public Service Management
PO–RALG	President's Office – Regional Administration and Local Government
POC	Point of Contact
PPF	Parastatal Pension Fund
PPRA	Public Procurement Regulatory Authority
PPP	Public-Private Partnership
R&D	Research and Development
RAHCO	Reli Assets Holding Company LTD
RITA	Registration Insolvency and Trusteeship Agency
SADC	Southern African Development Community
SEACOM	Southern and Eastern Africa Communications Network
SME	Small and Medium Enterprises
SOP	Standard Operating Procedures
SSL	Socket Security layer
SWOC	Strengths, Weakness, Opportunity and Challenges
TAA	Tanzania Airports Authority
TAMNOA	Tanzania Mobile Network Operators Association

Acronym	**Description**
TANESCO	Tanzania Electricity Supply Company
TANROADS	Tanzania National Roads Agency
TBS	Tanzania Bureau of Standards
TCAA	Tanzania Civil Aviation Authority
TCRA	Tanzania Communications Regulatory Authority
TCU	Tanzania Commission for Universities
TIC	Tanzania Investment Centre
TIE	Tanzania Institute of Education
TIRDO	Tanzania Industrial Research and Development Organization
TISPA	Tanzania Internet Service Providers Association
TIX	Tanzania Internet Exchange
TMA	Tanzania Meteorological Agency
TPA	Tanzania Ports Authority
TPC	Tanzania Postal Corporation
TPDF	Tanzania Peoples Defence Force
TPSF	Tanzania Private Sector Foundation
TPF	Tanzania Police Force
TR	Treasury Registrar
TRA	Tanzania Revenue Authority
TTCL	Tanzania Telecommunications Corporation
TZ-CERT	Tanzania Computer Emergency Response Team
TZNIC	Tanzania Network Information Centre (dot tz registry)
UCSAF	Universal Communications Services Access Fund
UNCTAD	United Nations Conference on Trade and Development
URT	United Republic of Tanzania
VPN	Virtual Private network

EXECUTIVE SUMMARY

Tanzania's National Cyber Security Strategy (NCSS) has been developed in the context of the National ICT Policy of 2016 (NICTP 2016), for the purpose of preparing the country to address the emerging cyber threats. Security of information resources and National Critical Information Infrastructure requires a coordinated approach that is systematic and holistic in nature. It calls for coordinated efforts between the government, private sector and civil society, and further requires regional and international collaboration, as well as information sharing related to Cyber Security. This Strategy, therefore, has been developed to ensure that the country operates in a safe and secure cyberspace.

The Government in its effort to address Cyber Security issues, has already taken some initiatives including enactment of the Cybercrimes Act, 2015; E-transactions Act, 2015 and the Electronic and Postal Communications Act, 2010 (EPOCA). The Government has also established the Computer Emergency Response Team (CERT), Central Equipment Identification Register (CEIR); and the Cybercrime Unit under the Tanzania Police Force. Despite these achievements and commitments, there are still challenges facing ICT Security which include ICT infrastructure vandalism as well as the unsecure usage of communication services which lead to cybercrime, infringement of privacy and detriment to national culture including child abuse online.

The development of this NCSS used a "focus groups" approach where a wide range of stakeholders from across the Cyber Security ecosystem participated in discussions and critical analysis of current Cyber Security posture of the URT. Additionally, the Cyber Security Capacity Maturity Model (CMM) was used to examine the Cyber Security maturity level in the country across five unique and key dimensions which are:-

1. Policy & Strategy;
2. Culture & Society;
3. Education, Training & Skills;
4. Legal & Regulatory Frameworks; and
5. Standards, Organisations, & Technologies.

This strategy is built on five guiding principles namely: Public-Private Partnerships; Ubiquitous threats; Risk based Management; Capacity Building and Awareness for All; plus Regional and International collaboration.

In-line with these principles, five strategic goals were formulated which include: Protection of Critical Information Infrastructure; Increase Cyber Security technical capabilities and awareness; Promote collaboration and information sharing on Cyber Security locally, regionally and internationally; Enhance incident response to address Cyber Security threats/trends; and enhance the legal and regulatory frameworks to ensure a secure cyberspace in Tanzania.

CHAPTER ONE

1. INTRODUCTION

1.1. Background

The global growth in Information and Communication Technologies (ICT) has greatly influenced human interactions and the way people live and conduct businesses. The rapid growth of ICT has greatly shaped human relations where societies seem to be more connected as a global village. Societies have steadily migrated from the traditional ways of transactions characterized by manual paper based processes to a fast evolving electronic world. This has strongly permeated the entire transaction spectrum seamlessly. Similarly, in Tanzania, the National ICT Policy 2003, which was revised in year 2016, provided a national framework for ICTs to contribute effectively towards achieving national development goals and transform Tanzania into a knowledge–based society through the application of ICT. This policy has facilitated the development of the Tanzanian ICT industry over the past years and has created a broad range of economic and social activities. For example, ICT has contributed to improvements in both public and private sector service delivery, which include formal and informal education, healthcare and various e-services. Additionally, the introduction of mobile money platforms in Tanzania has created new banking channels for people who previously did not have access to banking services. As a positive ripple, the Small and Medium Enterprises (SMEs) acting as mobile banking agents have created new forms of employment and livelihood.

While increased access to ICT and the Internet provide opportunities for social economic development, this rapid pace of technological innovation has resulted in incidents of cybercrime activities which are considered a major threat to economic development and national security worldwide. Cybercrime poses a direct threat to national security and the economy, and have profound effects on the daily lives of millions of citizens. While the National ICT Policy 2016 underscores the importance of Cyber Security, there is no formal Cyber Security strategy that articulates the country’s approach for addressing Cyber Security issues.

The Government of the URT recognizes that an effective response to cybercrime is important and must be holistic, involving multiple stakeholders. This approach considers all relevant sectors including Government, private sector and civil society in addressing cybercrimes effectively.

Therefore, within the context of the National ICT Policy of 2016 (NICTP 2016), the Government of the URT has developed this NCSS for a period of five years from 2018 until 2023 to describe the country's approach in ensuring a safe and secure cyberspace.

1.2. Scope

The NCSS scope addresses the activities and responsibilities of the Government, non-governmental stakeholders including communication and Internet service providers, civil society groups and the public in general. The Strategy addresses a number of Cyber Security areas of focus such as Protection of Critical Information Infrastructure; enhancement of Cyber Security technical capabilities and awareness; incident response; promotion of local, regional and international collaboration in Cyber Security; and enhancement of legal and regulatory frameworks to protect the cyber space.

1.3. Strategy Development Approach

Development of the NCSS used a "focus groups" approach in which a wide range of stakeholders from across Cyber Security ecosystem participated in discussion and critical analysis of current Cyber Security posture of the URT. In addition, the Cyber Security Capacity Maturity Model (CMM) was used to examine the maturity of Cyber Security in the country across five unique and key dimensions which are Policy & Strategy; Culture & Society; Education, Training & Skills; Legal & Regulatory Frameworks; and Standards, Organisations, & Technologies. A Strength, Weakness, Opportunity and Challenge (SWOC) analysis was also done in addition so as to attain the critical issues/focus areas.

1.4. The Layout and Structure of the Strategy

The strategy document is divided into a number of sections which include:

Chapter 1 is an introduction providing the background, scope of the strategy and the approach used in the development process.

Chapter 2 presents the current situation of the country's cyber well-fare; economically, politically, socially and technologically in order to identify factors influencing environment of the cyberspace and provide measures to safeguard it.

Chapter 3 provides the Plan which consists of the Mission, Vision, Goals, Guiding Principles Objectives, Strategies, Targets and Performance indicators. The chapter further describes the rationale for adopting the objectives and how to achieve them. Additionally, it describes governance structure for the implementation of the NCSS.

Annex 1 provides the matrix of the implementation strategy.

CHAPTER TWO

2. SITUATION ANALYSIS

This chapter elaborates the assessment of the current situation of the country's cyber well-fare; economically, politically, socially and technologically in order to identify factors influencing environment of the cyberspace and provide measures to safeguard it. In this Strategy, the Cyber Security Capacity Maturity Model (CMM) was used to examine the maturity of Cyber Security in the country across five unique and key dimensions which are Policy & Strategy; Culture & Society; Education, Training & Skills; Legal & Regulatory Frameworks; and Standards, Organisations, & Technologies. In addition, the government conducted an analysis of the external and internal environment of the cyber sphere of Tanzania, based on Strengths, Weakness, Opportunity and Challenges (SWOC) analysis and identified additional key major gaps. In this regard, highlights of the major strategic issues that are addressed through this Strategy have been presented. Both the SWOC and critical issues in regards to this strategy are meant to provide direction on the national efforts in ensuring a safe and secure cyberspace.

2.1 Policy and Strategy

This dimension of the analysis examines the capacity to resist and/or recover from cyber incidents based on existing national policies, strategies and plans. Under this dimension various factors that contribute to Cyber Security policy cohesion are reviewed to highlight existing efforts and gaps.

2.1.1 Official National Cyber Security Strategy

The National ICT Policy 2016 underscores the importance of Cyber Security and emphasizes that unsafe/unsecure use of communication services which results in negative impacts like cybercrime, infringement of privacy, damages to the national culture, and online child abuse is a big challenge. Various institutions in the country have Cyber Security initiatives in form of policies and plans for handling institutional cyber incidents, however, at the national level there is no documented Cyber Security strategy that details the country’s approach for addressing Cyber Security issues.

2.1.2 Incident Response

One of the major Cyber Security initiatives implemented by the Government of United Republic of Tanzania (URT) in recent years include the establishment and operationalisation of the Tanzania Computer Emergency Response Team (TZ-CERT). TZ-CERT was established under section 124 of the Electronic and Postal Communications Act (EPOCA) No 3/2010, and is responsible for:

i) Coordinating the national responses to Cyber Security incidents;

ii) Cooperating with regional and International entities involved with the management of Cyber Security incidents; and

iii) Identifying national level incidents and storing them in a central registry.

Despite the abovementioned efforts, there is still no comprehensive and formal framework to enable TZ-CERT coordinate and share information on cyber incidents at national, regional or international level. What's more, TZ-CERT has a limited capacity in terms of skills and infrastructure for detecting, managing, and responding to cyber incidents.

Another challenge is the current absence of a formally designated National Cyber Security Steering Committee or body/institution that is responsible for coordinating and overseeing Cyber Security issues in general.

Furthermore, there is no National Security Operation Centre (NSOC) to enable TZ-CERT and Tanzania Police Force (TPF) cybercrime unit to share, exchange and react to cyber incidents that might occur and cause damage to National Critical Information Infrastructure (CII).

2.1.3 National Critical Information Infrastructure (CII) Protection

The National ICT Policy of 2016 and the Cybercrimes Act, 2015 acknowledge the importance of CII. The Act mandates the Minister responsible for Communications by order published in the Gazette, to designate a computer system as CII.

In line with NICTP 2016, the Ministry of Works, Transport and Communication has put in place some initiatives to implement a National Public Key Infrastructure (NPKI) to enhance management of digital certificates and public-key encryption in the country.

Although there are a number of CII in various sectors such as Telecommunications, Banking and Utilities like power and water, there is no formal categorization of CII and thus there is no CII register. Another issue not properly addressed is that no national institution has been formally mandated to oversee the CII of the nation. As a result, there is a lack of formal collaboration mechanism between the government and owners of critical assets. Consequently, response planning is not handled in a formal or coordinated manner. It is also noted that there is no formal national Cyber Security governance structure to promote a multi-stakeholder approach for safeguarding the Nation's cyberspace.

2.1.4 Crisis Management

To manage crisis relating to ICT, public and private institutions established Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP). Some of these institutions have implemented the plans by having their own storage servers and conduct daily, weekly and monthly backup. Certain institutions such as BOT, TRA, e-GA and NIDA have built their own data centres. At a national level, the government through the Ministry responsible for ICT has built a modern data centre that serves both public and private institutions. The government has allocated 25% of the data centre’s resources to be used for public institutions and directed all the institutions to use the centre. The government has also established the Department of Records and Nation Archives (DRAM). This Department collects data relating to the government as hard copies, and converts these hard copies into electronic form and stores in both forms.

Despite these efforts, there are no redundancy systems in place at national level. Storage servers and data centers have not been replicated elsewhere and therefore if there is a physical destruction of the current server rooms and data centers then the data might be lost. Although individual institutions have BCP and DRP, the government has not developed its own BCP and DRP plans. As a result, there is no well established chain of command on reporting and reacting whenever there is a crisis.

2.2 Culture and society

This dimension examines the extent of awareness for relevant stakeholders on cyber risks, their use of the Internet safely and securely, and their inclination to take necessary steps to protect information resources.

2.2.1 Cyber Security mindset

Cyber Security mindset is a key to impart an information secure thinking to a human mind. The mindset in this context includes values, attitudes, practices and habits of the government, private sector and civil society at large in the Cyber Security ecosystem of the nation.

Generally, the mindsets of stakeholders have improved in recent years. The government through various Cyber Security programmes has positively influenced its organs and employees in terms of their attitude towards Cyber Security. For example, many of the government employees use government email systems to exchange work related documents. In addition, government employees adhere to the effective use of their passwords when logging into government related systems. Similarly, the private sector has also undertaken various steps towards encouraging a Cyber Security mindset in their staff and customers. For example, private bank and mobile operators send reminder and alert messages to their customers on the safe use of their pin codes via mobile phones. Furthermore, banks have installed special ATM keypad protection shields in their respective ATM machines. These and other similar initiatives have greatly improved the Cyber Security mindsets of the citizens at large.

However, not all citizens have been reached when it comes to changing Cyber Security mindsets. Some people live in the underserved areas where such services are not readily available. In addition, even some of those that have access to online services are hesitant to use them due to lack of trust.

2.2.2 Cyber Security Awareness

Cyber Security awareness of citizens plays a vital role in protecting information resources. This section examines the extent of stakeholders' awareness to Cyber Security with respect to cyber risks, threats and vulnerabilities across the nation.

There is considerable Cyber Security awareness among relevant stakeholder groups. From the government perspective, a number of awareness initiatives have been undertaken at a national level including awareness training programs to law enforcers, prosecutors, judges, magistrates and higher learning institutions on the Cybercrimes Act, 2015 and Electronic Transactions Act, 2015 and their implementation. Also, TZ-CERT sends out Cyber Security awareness building messages via multiple media such as social media. Furthermore, public academic institutions conduct various Cyber Security awareness programmes through their centres for continuing education. The private sector also provides Cyber Security awareness programmes across their respective lines of businesses

However, there is a lack of a coordinated national Cyber Security awareness raising programme. As a result, each stakeholder group handles Cyber Security awareness in their own ways.

2.2.3 Confidence and trust in online services

To effectively make use of online services, users require assurances on the security of their data online. This builds confidence and trust in online services. This sub-dimension focuses on the level of trust of users in online services.

Currently, some citizens enjoy access to various online services. Some of the services accessed online include access to pension fund contributions, access to academic results, payment of various utility bills, taxes, levies, application for admission into different higher learning institutions, application for higher education student loans, application for employment and registration of businesses. This shows that the level of confidence and trust in online services is increasing among citizens with adequate access to online services, though it is still relatively low among citizens in underserved areas.

Furthermore, some citizens are still uncertain on how their personal data are used or protected when they access online services hence are still hesitant in using online services.

2.2.4 Privacy online

Privacy issues include the sharing of personal data in public and private sector. This sub-dimension examines issues relating to the protection of personal data and online privacy at large.

The enactment of the Cybercrimes Act, 2015 and e-Transactions Act, 2015 demonstrate the government's effort to protect its citizens against abuses online, including abuses relating to privacy. There is also an ongoing initiative to enact a Data Protection Act which is specifically addressing the issue of protection of users' privacy online. In addition, the government through various initiatives has disseminated information regarding privacy online and user protection. Despite these efforts, not all online service users are well aware of the existence of the Cybercrimes and e-Transactions Acts of 2015. Furthermore, there is a lack of a comprehensive outreach programme to address online privacy aspects in the country.

2.3 Cyber Security Education, Skills and Training

This dimension examines the current state of Cyber Security training and education across the nation. Specifically, the dimension explores the actions undertaken by the government and academia to address aspects of capacity building in Cyber Security.

2.3.1 Availability of Cyber Security education

The country requires high quality Cyber Security education and training to ensure a sustainable supply of Cyber Security skills that cater to the needs of private and public sector. This sub-dimension assesses the efforts of the nation in ensuring availability of high quality Cyber Security education.

There are a number of Cyber Security training programmes across higher learning institutions in Tanzania. Also, the Tanzania Industrial Research and Development Organization (TIRDO) has established the ICT laboratory which provides training on Cyber Security and digital forensics. In addition, there are a number of Cyber Security certified professionals working with the government, public academic institutions and the private sector. Moreover, the URT has established the ICT Commission, which among other functions, is responsible for building capacity in ICTs, and promoting ICT professions in the country.

Notwithstanding all the above mentioned initiatives, Cyber Security is not included in the curriculum at lower levels of education such as primary and secondary schools. There are still relatively small numbers of Cyber Security certified professionals, and auditors who are specialized in Cyber Security in the country.

The country doesn't have an national agency to regulate Cyber Security certification standards, but currently public and private institutions have adopted international standards. In addition, there is no formally mandated government body or authority which is responsible for coordinating and managing Cyber Security education and/or certifications in Tanzania. Furthermore, there is no retention plan that has been developed by government that support retaining of the Cyber Security experts so as to address workforce challenges in both public and private sectors.

2.3.2 National Development of Cyber Security Education

This sub-dimension examines the extent of inclusion of Cyber Security education programmes in the national education strategy. Currently, the country is implementing the United Republic of Tanzania Education Sector Development Programme 2008 – 2017. The Commission for Science and Technology (COSTECH), Tanzania Industrial Research and Development Organization (TIRDO) and other public research and academic institutions are currently working on research projects that are related to ICT development. However, only a few of these projects focus on Cyber Security as the current National Research agenda does not explicitly address Cyber Security related Research and Development (R&D) aspects. Indeed, the URT Education Sector Development Programme 2008 - 2017 programme consider Cyber Security aspect as part of ICT.

2.3.3 Corporate Governance, Knowledge and Standards

This sub-dimension looks into the level of understanding of key stakeholder groups in dealing with Cyber Security risks, threats and vulnerabilities.

Some of the public and private institutions have information security policies and procedures in place. Furthermore, some institutions have introduced the post of an individual in-charge of information security. Such institutions include BOT, TRA, PPF, TTCL, eGA, TANESCO and NMB.

However, there is no harmonization of Cyber Security policies across all the MDAs and LGAs; and there is a need to introduce the post of an information security officer in-charge of Cyber Security across all public institutions in Tanzania. In addition, there is no national steering committee for managing the Cyber Security aspects in the country.

2.4 Legal and Regulatory Frameworks

This dimension seeks to analyse the current legal and regulatory frameworks relating to Cyber Security. In particular, the dimension reviews the current laws and regulations that are in place to deal with issues related to Cyber Security. Under this dimension various factors that relate to laws and regulations on Cyber Security are reviewed in order to identify existing efforts and gaps**.**

2.4.1 Cyber Security Legal Frameworks

In accordance with regional (SADC, EAC, AU) and international trends, nations are required to enact three main cyber legislations namely Cybercrimes, E-transactions and Personal Data Protection. Tanzania has so far promulgated the Cybercrimes Act, 2015 and the Electronic Transactions Act, 2015 which address issues like cybercrimes, e-commerce, e-government, e-signatures and e-contracts. The promulgation process of the Personal Data Protection Act has commenced and is ongoing. Tanzania has further developed Cybercrimes (general) Regulations, 2016 and Electronic Transactions (Cryptographic and Certification Services Provided) Regulations, 2016.

2.4.2 Legal Investigation and Prosecution

The capacity of the nation to combat cyber incidents, investigate and prosecute cybercrimes or other crimes using electronic evidence is crucial for effective implementation of the legal and regulatory framework. In Tanzania, there are three law enforcement agencies that are directly involved in the detection, investigation and prosecution of cybercrimes namely the Tanzania Police Force (TPF), the Director of Public Prosecution (DPP) and the Judiciary. Tanzania Police Force has established a Cybercrime Unit that deals with detection and investigations of Cybercrimes while DPP deals with prosecution of Cyber offences.

These law enforcement agencies (Judiciary, TPF and DPP) possess inadequate capacity in cybercrime investigation and prosecution. Though the Judiciary and DPP have extensive knowledge on prosecution of crimes, they lack some capacity in tackling Cybercrimes. Other gaps include the limited capacity of judges across the country in presiding over cases relating cybercrimes, or crimes requiring the use of electronic evidence. Another key gap is the current absence of a formal collaboration framework to promote collaboration between law enforcement, the judiciary and other stakeholders in the fight against cybercrimes.

2.4.3 Vulnerability Reporting

TZ-CERT is responsible for identifying, managing and responding to Cyber Security incidents at a national level. In order to facilitate reporting of incidents, TZ-CERT has categorized institutions of similar nature into Constituents. Each constituent may have sector-specific CERTs or sectoral CERTs, which serve these constituents. Therefore, if an incident occurs, the affected institution reports this incident to the corresponding sectoral CERT for assistance. Likewise, a sectoral CERT may request for assistance from the TZ-CERT. This is an effective reporting mechanism, however, additional sectoral CERTs (e.g. for Financial, Academia, Telecom etc) are yet to be formulated in order to enhance the TZ-CERT operations and functions.

2.5 Standards, Organizations and Technologies

This dimension examines the country's best practices in the acquisition, implementation and deployment of information systems and network infrastructure.

2.5.1 Adherence to Standards

This sub-dimension focuses on the ability of the nation to acquire and implement Cyber Security standards by public and private sector.

The Government has developed and published minimum requirements for acquisition of ICT equipment and Guidelines for appropriate, proper and safe usage of ICT based equipment and systems for its institutions. Also, the e-Government agency (eGA) has established and deployed a common emailing system for official use by public servants. Similarly, the Tanzania Communications Regulatory Authority (TCRA) has launched the Central Equipment Identity Register (CEIR) to enhance mobile phone security and detection of counterfeit handsets in the country. In addition, other public and private institutions have adopted and/or developed their own standards for safeguarding information resources.

Generally, the Tanzania Bureau of Standards (TBS) is the national organ that is responsible for setting up of standards for all products and services in the country.

However, TBS does not explicitly address Cyber Security standards neither does any other institution. There is also a lack of a specific body in the government that deals with setting up, adopting and governing Cyber Security related standards in the country. Furthermore, the information systems which are developed in-house have limited system design documentation which can result in challenges during technology transfers or troubleshooting of problems.

2.5.2 National Infrastructure Resilience

This sub-dimension examines how the nation deploys and manages information infrastructure to ensure reliability and resilience.

The deployment of the National Data Centre and National ICT Broadband Backbone (NICTBB) demonstrates the Government's efforts in ensuring that the Critical Information Infrastructure is reliable and resilient. Prior to the establishment of NICTBB, the National ICT Projects Steering committee was established to oversee the implementation of Nation ICT infrastructure projects. The NICTBB is deployed with bi-directional rings that can route the data traffic into the redundancy link in case faults occur across the primary links. Also, the NICTBB is implemented with Internet protocol/ Multi-Protocol Label Switching (IP/MPLS) that divert and route data traffic around link failures, congestion, and bottlenecks, as well as providing end-to-end data protection.

The NICTBB is connected with two submarine optical cables namely the Southern and Eastern Africa Communication Network (SEACOM) and the Eastern Africa Submarine cable System (EASSy) for transmitting international bandwidths. Similarly, there is a Tanzania internet exchange points (TIXs) that keeps local Internet traffic within NICTBB, and also reduces costs associated with traffic exchange between Internet Service Providers (ISPs) in the country. However, given the current network and national grid power infrastructure setups, there is inadequate redundancy in terms of both network infrastructure as well as power infrastructure in the country. Furthermore, there is no Single Internet Gateway for filtering Cyber Security incidents from other countries.

2.5.3 Online Marketplace

This sub dimension examines the extent of availability of online services or applications that can be acquired or developed locally.

A number of online applications have been developed and deployed, mainly by the private sector, to support business transactions in the country. These include MAXMALIPO, SELCOM, PUSHMOBILE, Nataka Gari, etc. Similarly, there are various institutions which have acquired online network security services such as Virtual Private network (VPN), IPSec and Socket Security layer (SSL) for protection of their information systems. However, the extent of the security of the applications and services provided is not certain.

2.6 Table1: SWOC Analysis

DIMENSIONS	INTERNAL ASPECTS		EXTERNAL ASPECTS	
	Strengths	**Weaknesses**	**Opportunities**	**Challenges**
Policy and Strategy	• Comprehensive National ICT Policy. • Existence of Information Security Policies, BCPs and DRPs at corporate level. • Existence of TZ-CERT. • Existence of storage facilities and/or data centres at institutional level. • Existence of Department of Records and National Archives	• Lack of National Cyber Security strategy. • Lack of Information Security Policies, BCPs and DRPs at national level. • Lack of a formally designated National CERT Steering committee. • Lack of the national Cyber Security strategy governance structure. • Lack of comprehensive and formal structure for reporting and reacting whenever there is a crisis. Lack of adequate skills and mechanism for detecting, managing, and responding to cyber incidents. • Lack of national institution to oversee CII. • Lack of National Security Operating Centre. • Lack of CII Registry. • Lack of redundancy systems in place at national level	• Availability of potential partners to collaborate in Cyber Security matters. • Existence of EAC Protocol on ICT Networks.	• Poor cooperation from external parties in Cyber Security matters. • Borderless nature of cybercrimes. • Difference in cross national legal frameworks in Cyber Security.

Culture and society	• Enactment of Cybercrimes Act, 2015 and E-Transactions Act, 2015. • Public and Private institutions awareness of cyber threats. • Existence of locally developed online services. • Availability of awareness programmes through public academic institutions and private sector.	• Lack of comprehensive national Cyber Security awareness and outreach programmes. • Lack of Data Protection Act. • Lack of local Cyber Security online services.	• Existence of international fora on Cyber Security issues.	• Ubiquitous nature of Cyber Security threats.

Cyber Security Education, Training and Skills	• Good political will. • Supportive leadership. • Existence of Cyber Security training programs in higher learning institutions. • Existence of ICT Commission. • Existence of research on ICT Development. • Existence of Cyber Security and Forensics lab – TIRDO. • Presence of Cyber Security certified professionals.	• Lack of national steering committee for Cyber Security. • Limited budget for Cyber Security aspects. • Lack of curriculum development guideline that includes Cyber Security aspects. • Lack of national research centre for Cyber Security. • Lack of Cyber Security aspects in the national research agenda. • Lack of a government body or authority for coordinating and managing Cyber Security certifications in Tanzania. • Inadequacy of Cyber Security certified professionals. • Lack of retention mechanism for Cyber Security experts. • Lack of local standard for Cyber Security certifications. • Lack of Cyber Security unit in most organizations.	• Availability of International certifications on Cyber Security. • Existence of international training on Cyber Security aspects. • Existence of research grants on Cyber Security. • Existence of regional and international Cyber Security R&D bodies.	• Reliance on external experts and technology solutions in the area of Cyber Security.

Legal and Regulatory Frameworks	• Existence of TCRA & TZ-CERT. • Supportive legal and regulatory framework (Electronic and Postal Communications Act, 2010 (EPOCA), Cybercrimes Act, 2015 and E-Transactions Act, 2015). • Existence of cybercrime unit (TPF – DPP). • Adoption of EAC, SADC and AU frameworks on cyber laws. • Existence of collaboration with regional and International organizations (AU, SADC, EAC, ITU, CTO, UNCTAD, EU etc).	• Inadequate Cyber Security skills in law enforcement agencies. • Lack of adequate mechanism to facilitate cooperation between law enforcers and other Cyber Security stakeholders. • Lack of adequate regional and international collaboration in Cyber Security. • Lack of comprehensive and formal structure for facilitating coordination and sharing of Cyber Security related information.	• Existence of EAC Protocol on ICT Networks.	• Borderless nature of cybercrimes. • Difference in cross national legal frameworks in Cyber Security.

Standards, Organizations and Technologies	• Existence of National ICT Projects Steering committee. • Existence of Central Equipment Identification Register (CEIR). • Existence of Tanzania Bureau of Standards (TBS) for setting up of standards for all products and services. Existence of the NICTBB • Existence of National Data Centre. • Existence of Internet exchange points (IXPs).	• Lack of national body for setting up, adopting and governing Cyber Security related standards. • Poor system documentation. • Lack of Cyber Security mechanism to control data in the cloud outside the country. • Lack of Cyber Security standards for acquisition of Information systems. • Lack of redundancy systems at national level. • Lack of a single national internet gateway.	• Availability of International standards and Best Practices on Cyber Security. • Availability of advanced technology or tools for detecting and investigating cybercrimes.	• Poor cooperation from external parties in Cyber Security matters. • Existence of malicious Cyber Security software/hardware tools. • Advanced nature of Hackers from • Malicious external individuals/organizations.

2.7 Critical Issues

i. Lack of comprehensive national Cyber Security awareness and outreach programmes.
ii. Unavailability of framework for identification and protection of CII
iii. Borderless nature of cybercrimes
iv. Ubiquitous nature of Cyber Security threats
v. Difference in cross national legal frameworks in Cyber Security
vi. Lack of Cyber Security units in most organizations
vii. Inadequate mechanisms for detecting, managing, and responding to cyber incidents

viii. Absence of Information Security Policies, BCPs and DRPs at national level
ix. Lack of the national Cyber Security strategy governance structure
x. Curriculum development guidelines that do not includes Cyber Security aspects
xi. Lack of Cyber Security aspects in the national research agenda;
xii. Lack of a government body or authority for coordinating and managing Cyber Security certifications;
xiii. Inadequate Cyber Security certified professionals
xiv. Insufficient Cyber Security skills in law enforcement agencies;
xv. Inadequate mechanism to facilitate cooperation between law enforcers and other Cyber Security stakeholders;
xvi. Inadequate regional and international collaboration in Cyber Security;
xvii. Lack of national body for setting up, adopting and governing Cyber Security related standards;
xviii. Ineffectiveness of formal structure for facilitating coordination and sharing of Cyber Security related information
xix. Malicious Actors
xx. Lack of National Public key Infrastructure (NPKI) and National Security Operating Centre (NSOC)

CHAPTER THREE

3. THE STRATEGY PLAN

This chapter presents the vision, mission, guiding principles, strategic goals, specific objectives, strategies, targets and performance indicators of the national Cyber Security strategy. The chapter further describes the rationale for adopting the objectives and how to achieve them. Additionally, it describes the governance structure including organization chart for the implementation of the strategy.

3.1 Vision:

"A nation with a secure, safe, resilient and trusted cyberspace"

3.2 Mission:

To build nation's capacity to secure and safeguard cyber space that supports an informed, knowledge-based, information-driven society, and enhances socio-economic development.

3.3 Guiding Principles

This Strategy is built on the following five principles in order to prepare the nation to handle Cyber Security incidents. These principles will underpin the successful implementation of the Strategy, and enable a safe and secure cyberspace.

3.3.1 Principle 1 - Multistakeholder Partnerships

This Strategy recognises that ensuring a secure and safe cyberspace which can be fully leveraged by URT is a shared responsibility of all ICT users within Tanzania including individuals, private and public sector organisations. The private sector in Tanzania owns and operates a larger share of critical information infrastructure. This infrastructure provides various services including payment of utility bills, communication, audio and video streaming services and other remittance services to citizens at large. This principle ensures there a collaborative effort by all ICT users in Tanzania, especially those within the public and private sectors, to better manage and mitigate Cyber Security risk across the nation, including across the National Critical Information Infrastructure.

3.3.2 Principle 2 - Ubiquitous threats

Threats to information resources and critical information infrastructure are ubiquitous. This principle takes into account the borderless nature of cyberspace, as well as the dynamic nature of cyber threats and vulnerabilities. As such, this Strategy will seek to ensure that new threats are adequately managed or addressed as they emerge.

3.3.3 Principle 3 - Risk based Management

To better mitigate the security risks a comprehensive risk assessment and vulnerability analysis should be carried out to ensure that the investment in the protection of information resources and critical infrastructure is aligned to national priorities, and commensurate with the value of the assets to be protected. Hence, this Strategy will ensure that the assessment of threats and risks, and the Cyber Security of the nation is risk based.

3.3.4 Principle 4 – Capacity building and Awareness for All

Information systems and critical information infrastructure fail not only because of technical flaws but also because of the low levels of Cyber Security awareness, as well as the lack of knowledgeable Cyber Security professionals. This Strategy will ensure that extensive Cyber Security capacity building and awareness building is undertaken across the nation, and these programmes are inclusive in nature to ensure all stakeholders are well informed and equipped to appropriately manage Cyber Security risks, threats and vulnerabilities.

3.3.5 Principle 5 - Regional and International collaboration

The nature of cyberspace is borderless and anonymous. With this perspective, Cyber Security threats and vulnerabilities are not limited to specific localities as, cyber criminal acts can cross various jurisdictions and borders. Therefore, regional and international collaboration is crucial to handling cybercrimes and Cyber Security incidents, and creating a more secure cyberspace ecosystem. This principle is meant to foster cross-border, Cyber Security information sharing, capacity building and regional coordination.

3.4 Strategic Goals

The National Cyber Security Strategy involve five strategic goals that are built within guiding principles and also have been formulated following extensively analysis of the external and internal environment (SWOC) contained in the cyber welfare of the country.

These strategic goals include:

1. Ensure protection of critical information infrastructure
2. Increase Cyber Security technical capabilities and awareness across Tanzania
3. Promote local, regional and international collaboration in Cyber Security
4. Enhance the national response to Cyber Security threats/trends
5. Enhance legal and regulatory frameworks to support Cyber Security initiatives in Tanzania

Goal 1: Ensure protection of critical information infrastructure

Rationale:

Critical information infrastructure according to the Cybercrimes Act 2015 include assets, devices, information systems, communication networks, whether physical or virtual so vital to the URT that their incapacitation affect national security or the economy and social well being of citizens. Protection of CII is therefore very important for security of the nation and for ensuring business continuity. Currently, there is no formal categorization of National Critical Information Infrastructure. As a result, it is difficult to define the different levels of protection of the respective Infrastructure. Since citizens are served by public as well as private service providers, both of which own some parts of the critical information infrastructure, there is a need for having a formal collaboration between private and public sector when it comes to protection of such infrastructure. This goal consists of strategies for achieving the continuous protection of the Critical Information Infrastructure.

3.4.1.1. **Specific objective 1:** Manage Critical Information Infrastructure (CII) in Tanzania

Strategies:

a) Establish a National Critical Information Infrastructure Register
b) Develop a National CII Governance Framework.
c) Establish a National Cyber Security Risk Register on CII
d) Develop regulations and/or guidelines that promote continuous risk assessment and management across CIIs in Tanzania
e) Promote and enhance regional and international cooperation in the protection of the Critical Information Infrastructure (CII)

Deliverables:

a) National CII Register
b) National CII Governance Framework
c) National Cyber Security Risk Register
d) Regional and international collaboration programmes
e) Regulations and/or guidelines

Key Performance Indicators:

a) Publication of National CII Register and frequency of updating the register
b) Publication of National CII Register governance framework
c) Frequency of update to National Risk Register
d) Publication of regulations and/or guidelines
e) Extent of international cooperation in the protection of CII

3.4.1.2. **Specific objective 2:** Improve the resilience, integrity and trustworthiness of CII in Tanzania.

Strategies:

a) Develop guidelines and/or regulations on hardware and software acquisition and usage.
b) Develop standard hardware and software specifications.
c) Establish National Public Key Infrastructure (NPKI).
d) Develop a National Contingency Plan for Tanzania
e) Develop and implement Cyber Security incident simulation scenarios and programs that can be used during the national exercises

Deliverables:

a) Guidelines and/or regulations and SOPs.
b) Specifications document.
c) NPKI
d) Cyber Security incident simulation scenarios and exercise programs
e) National Contingency Plan

Key Performance Indicators:

a) Extent of implementation of guidelines and/or regulations, SOPs
b) Approved Specifications document and extent of compliance of specifications.
c) Number of institutions using NPKI.
d) Number of incident simulation scenarios, exercises conducted and frequency of exercises

3.4.1.3. Specific objective 3: Enhance the mitigation of cyber threats and vulnerabilities

Strategies:

a) Monitor and manage cyber threats and vulnerabilities
b) Undertake system audits

Deliverables:

a) Cyber threats and vulnerabilities and penetration test reports
b) National Security Operating Centre (NSOC)
c) Audit reports

Key Performance Indicators:

a) Number of threats and vulnerabilities and penetration tests
b) Operational NSOC
c) Number of threats and vulnerabilities detected and prevented by NSOC
d) Number of audit queries and system audits, and frequency of system audits

Goal 2: Increase Cyber Security technical capabilities and awareness across Tanzania

Rationale:

Ensuring Cyber Security nationwide will consist of protecting computers, networks, information systems and data from unintended or unauthorized access, changes or damages. To successfully accomplish this, concerted efforts from all stakeholders starting from infrastructure owners, administrators, users, and other implied beneficiaries are required. This will require the development of technical capabilities which would involve specialised technical training, and non-technical aspects that require awareness building programmes. That is why there is a need to have proper Cyber Security capacity building and awareness programmes for respective groups of stakeholders.

3.4.2.1. Specific Objective 1: Enhance cyber defence capability against cyber attacks in Tanzania

Strategies:

a) Build capacity on Cyber Security across the CERT and other relevant institutions
b) Develop internship and mentorship programmes among academic institutions and relevant stakeholders.

c) Develop national capacity on digital forensics
d) Establish relevant Cyber Security cadre in Public Service
e) Develop curriculum guidelines that promote the inclusion of Cyber Security in all national curricula
f) Develop career progression and retention policy relating to Cyber Security cadre
g) Create awareness on security features of IPV6 and prepare for transition from IPV4 to IPV6

Deliverables:

a) Cyber Security training and awareness programmes
b) Forensics Analysis and Investigation Training programme
c) Revised schemes of service
d) Revised curriculum guideline
e) Career Progression and Retention Policy
f) IPV6 awareness and implementation programmes

Key Performance Indicators:

a) Number of personnel trained and frequency of Training sessions
b) Approved schemes of service and number of Cyber Security personnel
c) Number of institutions with revised curricula and certifiable competence Level
d) Approved policy on career progression and retention and labour turnover
e) Number and frequency of awareness programs conducted and implementation of IPV6

3.4.2.2. **Specific Objective 2:** Promote research and development in Cyber Security in Tanzania.

Strategies:

a) Revise the National Research Agenda to include Cyber Security
b) Support Cyber Security competitions and R & D projects in Academic institutions and enterprises
c) Establish a National Cyber Security R&D Centre (NCRC)

Deliverables:

a. Revised National Research Agenda
b. Cyber Security competitions and R&D supporting framework, and Competition programmes and projects
c. National Cyber Security R&D Centre (NCRC)

Key Performance Indicators:

a) Approved Revised National Research Agenda and number of research and publications on Cyber Security

b) Number of research proposals and publications, competitions and Cyber Security solutions,

c) NCRC established

3.4.2.3. Specific Objective 3: Promote Cyber Security awareness across all segments of society in Tanzania.

Strategies:

a) Create a specialized outreach programmes including programmes that target children and other vulnerable groups

b) Establish a National Cyber Security Day in Tanzania

c) Develop national roadmap for improving Cyber Security awareness

Deliverables:

a) Outreach Programmes

b) National Cyber Security Day

c) Cyber Security awareness roadmap

Key Performance Indicators:

a) Level of awareness (% target groups), number of people reached and frequency of programmes

b) Established National Cyber Security Day and nationwide Activities to mark the day

c) Approved roadmap

Goal 3: Promote local, regional and international collaboration in Cyber Security

Rationale:

The nature of cyberspace is borderless and anonymous. With this perspective, Cyber Security threats and vulnerabilities are not limited to specific localities as, cyber criminal acts can cross various jurisdictions and borders. Therefore, regional and international collaboration is crucial to handling cybercrimes and Cyber Security incidents, and creating a more secure cyberspace ecosystem. This principle is meant to foster cross-border, Cyber Security information sharing, capacity building and regional coordination.

3.4.3.1. Specific Objective 1: Enhance local collaborations in Cyber Security

Strategies:

a) Develop a national governance and collaboration framework on Cyber Security

b) Conduct tracer studies among Academic institutions and relevant stakeholders

c) Create national fora to promote information sharing

d) Strengthen TZ-CERT for overseeing cooperation and collaboration on Cyber Security

e) Develop national exchange programmes to facilitate exchange of expertise on Cyber Security
f) Facilitate the creation of national partnerships framework to promote R&D in Cyber Security

Deliverables:

a) National governance & collaboration framework on Cyber Security
b) Mentorship and internship programmes
c) Tracer study reports
d) National Fora
e) Strengthen TZ-CERT for cooperation and collaboration on Cyber Security
f) Expertise exchange programmes
g) National Partnerships on R&D in Cyber Security

Key Performance Indicators:

a) Approved framework and number of joint activities
b) Number of mentorship and internship programmes on Cyber Security created, and graduates enrolled into the programmes.
c) Number of tracer study reports and academic institutions that have conducted tracer study
d) Number of national fora and institutions participating
e) Strengthen TZ-CERT and number of institutions collaborating
f) Number of exchange programmes and experts taking part in these programmes
g) Number of national partnerships on R&D

3.4.3.2. **Specific Objectives 2:** Promote regional and international collaborations in Cyber Security

Strategies:

a) Develop a regional and international collaboration framework
b) Develop internship and mentorship programmes with regional and international stakeholders
c) Participate regional and international fora to promote information sharing on Cyber Security
d) Develop programmes for Regional and International exchange of expertise on Cyber Security
e) Facilitate the creation of regional/international partnerships frameworks to promote R&D in Cyber Security
f) Promote adoption and adherence to regional and international standards and Best Practices on Cyber Security

Deliverables:

a) Regional and International Collaboration framework
b) Mentorship and internship programmes

c) Established regional and international fora
d) Regional and International expertise exchange programmes
e) Number of international partnerships on R&D
f) Regional and international standards and Best Practices

Key Performance Indicators:

a) Approved framework, and number of joint activities and MoU signed
b) Number of mentorship and internship programmes on Cyber Security created
c) Level of participation in Regional and International Fora
d) Number of international exchange programmes and experts participating in projects
e) Number of research proposals and publications
f) Number of standards and Best Practices

Goal 4: Enhance the national response to Cyber Security threats/trends

Rationale:

One of the efforts made by the Government in addressing cyber incidents is the establishment of the Tanzania Computer Emergency Response Team (TZ-CERT) under section 124 of the Electronic and Postal Communications Act (EPOCA) no. 3/2010 within the structure of Tanzania Communication Regulatory Authority (TCRA). TZ-CERT is responsible for coordinating responses to Cyber Security incidents at the national level, and cooperating with regional and International entities involved with the management of Cyber Security incidents. However, and to date, there is no formal coordination framework to enhance, and ensure an effective national response to Cyber Security threats and trends. Consequently, there is a need to improve the effectiveness of the national response to cyber threats and trends, and this will include enhancing various frameworks relating to Cyber Security governance, incident response, information sharing, etc.

3.4.4.1. **Specific Objective 1:** Promote incident response reporting and analysis in Tanzania

Strategies:

a) Develop incident reporting and information sharing framework
b) Develop standard log requirements
c) Continuously update the Cyber Security incidents register
d) Assess incidents and implement remedial measures
e) Develop risk mitigation measures

Deliverables:

a) National Incident reporting and information sharing framework
b) Standard log requirements
c) Cyber Security incidents register

d) Incidents assessment reports and remedial measures
e) risk mitigation measures

Key Performance Indicators:

a) Approved framework, and extent of Incident reporting and information sharing
b) Approved standard log requirements, and number of institutions adhering to standard log requirements
c) Frequency of updating incidents register
d) Number of incidents assessed, number of remedial measures taken, and frequency of incidents assessment
e) Number of risks mitigated

3.4.4.2. **Specific Objectives 2:** Enhance Cyber Security governance structures

Strategies:

a) Establish National Cyber Security Steering Committee
b) Develop Cyber Security coordination framework
c) Institutionalize Cyber Security governance structures and processes
d) Establish a Cyber crisis management unit

Deliverables:

a) National Cyber Security Steering Committee
b) Coordination framework
c) Cyber Security institutionalization document
d) Cyber crisis management unit

Key Performance Indicators:

a) Approved National Cyber Security Steering Committee
b) Approved framework
c) Approved institutionalization document
d) Approved Cyber crisis management unit and number of crisis resolved

Goal 5: Enhance legal and regulatory frameworks to support Cyber Security initiatives in Tanzania

Rationale:

Tanzania intends to have a secure, safe, resilient and trusted Cyberspace. To achieve this vision, there should be proper legal and regulatory frameworks that create a conducive environment for the safe and secure use of cyberspace, facilitate the enforcement of relevant laws, and enable effective investigation and prosecution of cybercrimes.

3.4.5.1. **Specific Objective 1:** Strengthen legal and regulatory framework to address Cyber Security

Strategies:

a) Review relevant Policies and Legislations
b) Develop legislations to enable and facilitate Cyber Security initiatives

c) Develop guidelines to protect vulnerable groups from cyber threats

Deliverables:

a) Comprehensive policies and legislations
b) Data Protection Act; Consumer Protection Act; Child Online Protection legislation; and any other relevant legislation.
c) Guidelines to protect vulnerable groups

Key Performance Indicators:

a) Number of amended legislations and revised policies.
b) Number of legislations enacted
c) Approved guidelines and number of vulnerable groups protected.

3.5 Governance Structure, Key Stakeholders and Resources for Implementing the Strategy

The governance structure presented in this section responds to the thrust of the Cyber Security strategy, which identifies and defines the roles and responsibilities of various actors. Considering that implementation of this Strategy is only possible through participation of all key stakeholders, the identification and definition of their roles is inevitable. The common and shared vision, mission, goals and objectives as clearly defined in this strategy will have to be realized if key stakeholder will play their specific roles. In that case, enhancement of public-private partnership (PPP) promoting *"a nation with a secure, safe, resilient and trusted cyberspace"* will be pre-requisite.

Effective governance structure is needed to facilitate players in providing access to information and knowledge to all citizens and institutions (public and private) and thus promoting performance improvement in cyberspace. For sustainable implementation of the Cyber Security strategy, each stakeholder in the envisaged arrangement has a role to play; the key institutions and their responsibilities are stipulated below in the proposed governance structure.

4. Key Stakeholders

The roles and responsibilities of various stakeholders involved in Cyber Security in the country has been established based on sector Policies, Laws and Regulations. The laws in consideration include: the Electronic and Postal Communication Act (EPOCA) 2010; the Cybercrimes Act, 2015; The E-transactions Act, 2015 and other Acts establishing individual institutions as follows in Table 2.

Table 2: Key Stakeholders' responsibilities

S/N	INSTITUTION	RESPONSIBILITIES
1.	Ministry Responsible for ICT	i. Prepare and Review policies, legislations and regulations ii. Oversee implementation of the strategy iii. Monitor and evaluate implementation of policies and strategies
2.	TZ-CERT	i. Coordinate the National Cyber Security issues; ii. Cooperate with Regional and International entities involved with management of cyber security incidents; iii. Identify national level incidence and storing them iv. To proactively provide early warning on eminent Cyber Security incidents; v. Participate on development and implementation of Cyber Security incident simulation scenarios and programs; vi. Monitor and manage Cyber threats and vulnerabilities; vii. Develop National roadmap for improving Cyber Security awareness; viii. Maintain a trusted National focal Point of Contact (PoC) within and beyond the national boarders that responds to Cyber Security incidents; ix. Participate on development of a regional and international collaboration framework; x. Create fora to promote information sharing on Cyber Security; xi. Create and update Cyber Security incidents register; xii. Assess incidents and implement remedial measures; xiii. Detect and disseminate information related to Cyber Security incidents;

S/N	INSTITUTION	RESPONSIBILITIES
		xiv. To handle and monitor Cyber Security incidents

3.	Law Enforcers	Law enforcement will be represented by the Police, Judiciary and Director of Public Prosecution. Their role are as follows:-
		i. Detection;
		ii. Investigation;
		iii. Prosecution ;

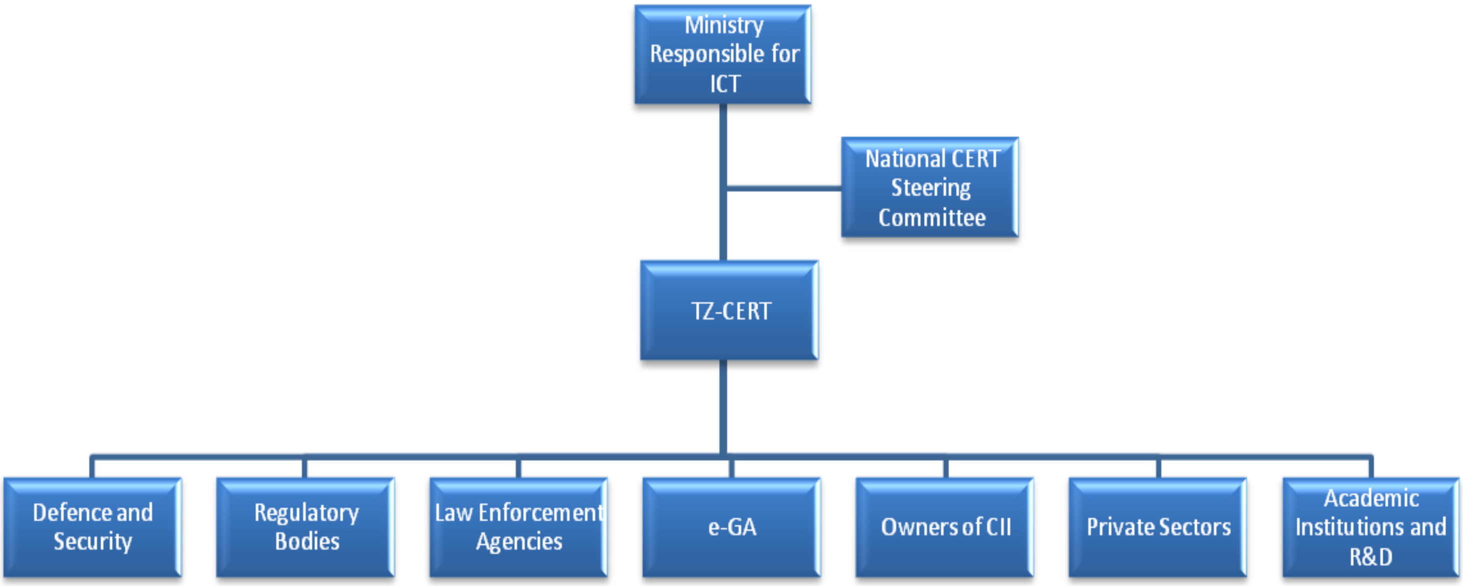
4.	Regulatory Bodies (TCRA, BOT, TBS, ICT Commission)	The regulators shall be responsible for enforcement of laws and regulations relating to Cyber Security

5.	Owners of Critical Information Infrastructure	TRA, NIDA, RITA, TANESCO, TPDF, TPF, TTCL, FINANCIAL INSTITUTIONS, RAHCO, MNOs, Immigration Department, TANROADS, BRT, National Archives, Po-PSM, Treasury, BoT, TCAA, TAA, TPA, TMA, TCRA, Ministry of Health., PO-RALG, MWTC, eGA , DAWASA, TCU, HESLB, NECTA.
		i. Facilitate identification;
		ii. Prioritization;
		iii. Assessment;
		iv. Protection of critical information infrastructure

6.	Private Sector	Private sector own and operate infrastructure and information systems that provide services to the government and citizens. They have the following responsibilities: i. Install, operate and manage secure networks ii. Provide reliable services to the citizens iii. Create Cyber Security awareness to the end users iv. Report risk associated with systems/networks
7.	Academic institutions and R&D	The academia will constitute Universities, Colleges, Tertiary and Research and Development Institution. The roles of the

S/N	INSTITUTION	RESPONSIBILITIES
		academia will be as follows: i. Develop competent human capital; ii. Capacity building on Cyber Security; iii. Review education curriculum; iv. Conduct joint research on Cyber Security; and v. Support Cyber Security R&D projects in Academic institutions and enterprises.
8.	Defence and Security Organs	Defence and Security Organs will be represented by TPDF, TISS, TPF and Immigration. Their roles are as follows:- i. Defend National Critical Information Infrastructure ii. Ensure freedom of action in National cyberspace and denial of the same against adversaries
9.	e-GA	i. Prepare Policy and Regulations regarding Government Infrastructure Security ii. Monitor and Evaluate, protect critical Infrastructure for Government use

5. Proposed Governance Structure



6. Resources for Implementing the Strategic Plan

As Tanzania is heading towards transformation to a knowledge society relying heavily on the use of ICTs, Cyber Security is a basic prerequisite for smooth operations of every organisation both public and private. MDAs and LGAs will therefore need to set aside budgets for supporting Cyber Security in their organisations in the same way they do for other business aspects. This means that each organisation will have to consider Cyber Security and make adequate budgetary provisions to ensure business continuity. Key stakeholders in Cyber Security strategy based on their role will be required to consider and undertake the tasks of Cyber Security and activities as spelt out in this strategy and include them in their budgets. Nevertheless, for enhancing the capacity of the nation to detect and manage Cyber Security threats and incidents, a budget will be set aside for supporting capacity building programmes and acquisition of state of the art equipment. A special budgetary provision will also be made to cover human resources development through the ministries responsible for ICT and Education. Another area that will need special budgetary provision is the enhancement of capabilities of detecting and managing Cyber Security threats and incidents at the Tz-CERT, and cybercrime units within TPF.

7. ANNEX 1: Matrix of the implementation of the National Cyber Security Strategy (NCSS)

Specific Objectives	Strategies/ Actions	Deliverables / Outputs	Lead Organization	Responsible Organizations	Time Frame	Key Performance Indicators
	Strategic Goal – 1: Ensure the protection of critical information infrastructure					
Manage CII in Tanzania	Establish a National Critical Information Infrastructure Register	National CII Register	TZ-CERT	MWTC, TTC	Within 6 months	Publication of National CII Register Frequency of updating the register
	Develop a national CII Governance Framework	National CII Governance Framework	MWTC	MWTC, TTC, TCRA,	Within 6 months	Publication of National CII Register governance framework
	Establish a National Cyber Security Risk Register on CII	National Cyber Security Risk Register	TZ-CERT		Within 6 months	Frequency of update to National Risk Register
	Develop regulations and/or guidelines that promote continuous risk assessment and management across CIIs in Tanzania	Regulations and/or guidelines	MWTC	MWTC, TTC, TCRA, AGC,	Within 6 months	Publication of regulations and/or guidelines
	Promote and enhance regional and international cooperation in the protection of the critical information infrastructure (CII)	Regional and international collaboration programmes	TCRA	MWTC, TCRA, TTC	Within 12 months	Extent of international cooperation in the protection of CII
Improve the resilience and	Develop guidelines	Guidelines and/or	TCRA	MWTC, TTC, TCRA, AGC,	Within 6 months	Extent of implementation

Specific Objectives	Strategies/ Actions	Deliverables / Outputs	Lead Organization	Responsible Organizations	Time Frame	Key Performance Indicators
integrity of CII in Tanzania	and/or Regulations on hardware and software acquisition and usage	regulations and SOPs				of guidelines and/or regulations, SOPs,
	Develop standard hardware and software specifications	Specifications document	IGC, TCRA	MWTC, TTC, TCRA, AGC,	Within 6 months	Approved Specifications document Extent of compliance of specifications
	Establish National Public Key Infrastructure (NPKI)	NPKI	TCRA	MWTC,IGC, E-GA, BOT, TPC	Within 18 months	Number of institutions using NPKI
	Develop and implement Cyber Security incident simulation scenarios and programs that can be used during the national exercises	Cyber Security incident simulation scenarios and exercise programs	TZCERT		Within 12 months	Number of incident simulation scenarios Number of exercises conducted Frequency of exercises
Enhance mitigation of cyber threats and vulnerabilities	Monitor and manage cyber threats and vulnerabilities	Cyber threats and vulnerabilities reports Penetration test reports	TZCERT		Within 3 months	Number of threats and vulnerabilities Number of penetration tests
	Establish National Network Security	NSOC	TCRA		Within 24 months	Established NSOC Number of threats and

Specific Objectives	Strategies/ Actions	Deliverables / Outputs	Lead Organization	Responsible Organizations	Time Frame	Key Performance Indicators
	Operating Centre (NSOC)					vulnerabilities detected and prevented by NSOC
	Undertake System audits	Audit reports	TZ-CERT		Within 12 Months	Number and frequency of system audits Number of audit queries
	Strategic Goal – 2: Increase the Cyber Security technical capabilities, and awareness across Tanzania					
Enhance cyber defence capability against cyber attacks in Tanzania	Build capacity on Cyber Security	Cyber Security training and Awareness programmes	MWTC	MOJCA, MOHA, TPDF, TPF, MOEST & All MDAs and LGAs	Within 3 months	Number of personnel trained Frequency of training sessions
	Develop national capabilities for forensics analysis	Forensics Analysis and Investigation Training programme	MWTC	MOHA MOJCA, TPDF, TPF, AGC, TZCERT, DPP, Judiciary	Within 12 months	Number of personnel trained Frequency of Training sessions
	Establish relevant Cyber Security cadre in Public Service	Revised schemes of service	POPSM	MWTC, TR, MOEST, MOFEA	Within 12 months	Approved schemes of service Number of Cyber Security personnel
	Develop curriculum guideline that demand inclusion of Cyber Security as cross cutting competence in	Revised curriculum guideline	MOEST	TCU, NACTE, TIE, Academic institutions, MWTC	Within 18 months	Number of institutions with revised curricula Certifiable competence Level

Specific Objectives	Strategies/ Actions	Deliverables / Outputs	Lead Organization	Responsible Organizations	Time Frame	Key Performance Indicators
	all curricula					
	Develop Career Progression and Retention Policy relating to Cyber Security cadre	Career Progression and Retention Policy	POPSM	MWTC, MOFEA	Within 18 months	Approved policy on career progression and retention Labour turnover
	Create awareness on security features of IPV6 and prepare for transition from IPV4 to IPV6	IPV6 awareness programmes	TzNIC	TCRA	Within 6 months	Number and frequency of awareness programs conducted
Promote research and development in Cyber Security in Tanzania	Revise the National Research Agenda to include Cyber Security	Revised National Research Agenda	COSTECH	MWTC, MOEST, Academic and Research Institutions	Within 12 months	Approved Revised National Research Agenda Number of research and publications on Cyber Security
	Support Cyber Security competitions and R & D projects in Academic institutions and enterprises	Cyber Security competitions and R&D supporting framework Competition programmes and projects	COSTECH	MWTC, MOEST, Academic and Research Institutions	Within 12 months	Number of research proposals Number of research and publications Number of competitions Number of Cyber Security solutions
	Establish a National Cyber Security R&D Centre (NCRC)	NCRC	MWTC	COSTECH, TR, TPDF, TPF	Within 18 months	Approved NCRC establishment proposal NCRC

Specific Objectives	Strategies/ Actions	Deliverables / Outputs	Lead Organization	Responsible Organizations	Time Frame	Key Performance Indicators
						Established
Promote Cyber Security awareness across all segments of society in Tanzania	Create a specialized outreach programmes	Outreach Programmes	MWTC	TZCERT, PORALG, TPF, MOICSA, MOAT	Within 6 months	Level of awareness (% target groups) Number of people reached Frequency of programmes
	Establish a National Cyber Security Day in Tanzania	National Cyber Security Day	MWTC	MOICSA, TZCERT, MOAT	Within 6 months	Established National Cyber Security Day Nationwide Activities to mark the day
	Develop National roadmap for improving Cyber Security awareness	Cyber Security awareness roadmap	MWTC	MOICSA, TZCERT, MOAT	Within 12 months	Approved roadmap
	Strategic Goal – 3: Promote local, regional and international collaboration in Cyber Security					
Enhance local collaborations in Cyber Security	Develop local collaboration framework	Local collaboration framework	MWTC	POPSM, eGA, MOEST, TPSF and all other Public and Private institutions	Within 12 months	Approved framework Number of joint activities
	Develop internship and mentorship programmes among Academic institutions and relevant stakeholders	Mentorship and internship programmes.	MOEST	MWTC, POPSM, COSTECH, MOLE, TPSF, TIC, MOIT, Academic institutions,	Within 12 months	Number of mentorship and internship programmes on Cyber Security created; Number of graduates enrolled into the programmes.

Specific Objectives	Strategies/ Actions	Deliverables / Outputs	Lead Organization	Responsible Organizations	Time Frame	Key Performance Indicators
	Conduct tracer studies among Academic institutions and relevant stakeholders	Tracer study reports	MOEST	MWTC, COSTECH, POPSM, TPSF, Academic Institutions	Within 18 months	Number of tracer study reports. Number of academic institutions that have conducted tracer study.
	Create national fora to promote information sharing	National Fora.	MWTC	TZCERT, eGA, MOICSA, TPF, TPDF	Within 9 months	Number of National Fora. Number of institutions participating.
	Establish or appoint a national body for overseeing cooperation and collaboration on Cyber Security	strengthening body for cooperation and collaboration on Cyber Security	MWTC	ICTC, TZCERT, TPF, TPDF, eGA	Within 12 months	Established National body Number of institutions collaborating
	Develop programmes to facilitate exchange of expertise on Cyber Security	Expertise exchange programmes.	MWTC	TPF, TPDF, POPSM, TZCERT, eGA, Academic institutions, TAMNOA TPSF, TISPA	Within 6 months	Number of programmes. Number of experts.
	Conduct joint research on Cyber Security	Joint research	COSTECH	MWTC, MOEST, TZCERT, Academic Institutions	Within 6 months	Number of research proposals. Number of research and publications.
Promote regional and international collaborations in Cyber Security	Develop a regional and international collaboration framework	Regional and International Collaboration framework	MWTC	TZCERT, TPF, TPDF, MOFAEAC, POPSM, eGA, MOEST, TPSF and all other Public and Private	Within 12 months	Approved framework Number of joint activities Number of MoU signed

Specific Objectives	Strategies/ Actions	Deliverables / Outputs	Lead Organization	Responsible Organizations	Time Frame	Key Performance Indicators
				institutions		
	Develop internship and mentorship programmes with regional and international stakeholders	Mentorship and internship programmes	MOEST	MWTC,MOFAEAC, POPSM, COSTECH, MOLE, TPSF, TIC, MOIT, Academic institutions	Within 12 months	Number of mentorship and internship programmes on Cyber Security created;
	Create regional and international fora to promote information sharing on Cyber Security	Regional and International Fora.	TZ-CERT	MWTC MOFAEAC, eGA, MOICSA, TPF, TPDF	Within 12 months	Number of Regional and International Fora. Number of institutions participating
	Develop programmes for Regional and International exchange of expertise on Cyber Security	Regional and International expertise exchange programmes	MWTC	MOFAEAC, TPF, TPDF, POPSM, TZ-CERT, eGA, Academic institutions, TAMNOA TPSF, TISPA	Within 12 months	Number of programmes. Number of experts.
	Conduct Regional joint research on Cyber Security.	Regional joint research	MWTC	MOEST, MOFAEAC, COSTECH, TZCERT, Academic Institutions	Within 6 months	Number of research proposals. Number of research and publications.
	Realization, Compliance and adherence to regional and international standards and Best Practices on Cyber Security	Regional and international standards and Best Practices	MWTC	TZCERT, TCRA, TPF, TPDF, eGA, MOFAEAC, TPSF, Academic Institutions MOIT,	Within 12 months	Number of standards and Best Practices
	Strategic Goal – 4: Enhance incident response to address Cyber Security threats/trends					
Promote incident response reporting and	Develop incident reporting and information	National Incident reporting and information	TZCERT	MWTC, eGA, POPSM, TPF, TPDF, TR, TPSF, Academic	Within 6 months	Approved framework Extent of

Specific Objectives	Strategies/ Actions	Deliverables / Outputs	Lead Organization	Responsible Organizations	Time Frame	Key Performance Indicators
analysis in Tanzania	sharing framework	sharing framework		Institutions		Incident reporting and information sharing
	Develop standard log requirements	Standard log requirements	TZCERT	MWTCTPF, TPDF, PPRA, POPSM, eGA, TPSF, Academic Institutions	Within 6 months	Approved standard log requirements Number of institutions adhering to standard log requirements
	Update Cyber Security incidents register	Cyber Security incidents register	TZCERT	MWTC,	Within 3 months	Frequency of updating incidents register
	Assess incidents and implement remedial measures	Incidents assessment reports Remedial measures	TZCERT	MWTC, ICTC, TPF, TPDF, TISPA eGA, Academic Institutions, TPSF,	Within 3 months	Number of incidents assessed Number of remedial measures taken Frequency of incidents assessment
	Develop risk mitigation measures	risk mitigation measures	TZCERT	MWTC, ICTC, TPF, TPDF, eGA, Academic Institutions, TPSF, TISPA	Within 6 months	Number of risks mitigated
Enhance Cyber Security governance structures and processes	Establish National Cyber Security Steering Committee	National Cyber Security Steering Committee	MWTC	TPF, PO, TPDF, PMO, MOHA, MODNS, MOEST, MOFP, MOFAEAC	Within 18 months	Approved National Cyber Security Steering Committee
	Develop Cyber Security	Coordination framework	MWTC	TZCERT, ICTC	Within 6 months	Approved framework

Specific Objectives	Strategies/ Actions	Deliverables / Outputs	Lead Organization	Responsible Organizations	Time Frame	Key Performance Indicators
	coordination framework					
	Institutionalize Cyber Security governance structures and processes	Cyber Security institutionalization document	MWTC	TPF, PO, MOFAEAC TPDF, PMO, MOHA, MODNS, MOEST, MOFP,	within 12 months	Approved institutionalization document
	Establish a Cyber crisis management unit	Cyber crisis management unit	POPSM	MWTC, TZCERT, MOHA, MODNS, TPDF, TPSF, TPF	within 6 months	Approved Cyber crisis management unit Number of crisis resolved
	Strategic Goal – 5: Enhance legal and regulatory framework to support Cyber Security initiatives in Tanzania					
Strengthen legal and regulatory framework for Cyber Security initiatives	Review relevant Policies and Legislations	Comprehensive policies and legislations	MWTC,	AGC, MOJCA, LRC, TPF	Within 12 months	Number of amended legislations Number of revised policies
	Develop legislations to support Cyber Security initiatives	Data Protection Act Consumer Protection Act Child Online Protection legislation Any other relevant legislations	MWTC	AGC, MOJCA, TPF, LRC, DPP, FCC, MOICSA, MOEST	Within 12 months	Number of legislations enacted
	Develop guidelines to protect vulnerable groups from cyber threats	Guidelines to protect vulnerable groups	MWTC	AGC, MOJCA, TZCERT, TPF, LRC, DPP, MOICSA, MOEST, TPSF, TAMNOA, Academic institutions	Within 6 months	Approved guidelines Number of vulnerable groups protected