THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE

GOVERNMENT CYBER SECURITY STRATEGY 2022

Scan to Read Online

THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE

GOVERNMENT CYBER SECURITY STRATEGY 2022

Scan to Read
Online

Publication data

President's Office,
Public Service Management and Good Governance,
Government City,
P.O BOX 670,
DODOMA,
Tanzania.

Email: ps@utumishi.go.tz
Phone No: **+255 262 160 240**
Mobile No: **+255 734 986 508**
Website: **www.utumishi.go.tz**

TABLE OF CONTENTS

LIST OF TABLES

ABREVIATIONS AND ACRONYMS

4IR	Fourth Industrial Revolution
API	Application Programming Interface
CCM	Chama Cha Mapinduzi
CMVRS	Central Motor Vehicle Registration System
DSM	Dar-es-Salaam
EGA	e-Government Authority
eGovRIDC	e-Government Authority-Government Research, Innovation and Development Center
FYDP III	Third National Development Plan
GDC	Government Data-centre
GDSXP	Government Data Exchange Platform
GDP	Gross National Product
GeOS	Government e-Office System
GePG	Government e-Payment Gateway
GMS	Government Mailing System
GOT	Government of Tanzania
GovNet	Government Network
GSD	Government Services Directory
HCMIS	Human Capital Management Information System
ICT	Information and Communication Technology
KPI	Key Performance Indicators
LAN	Local Area Network
LGA	Local Government Authority
MDAs	Ministries, Independent Departments and Executive Agencies
mGov	Mobile Government Platform
PO-PSMGG	President's Office, Public Service Management and Good Governance
PO-RALG	President's Office, Regional Administration and Local Government
TR&I	Technology Research and Innovation
TDV-2025	Tanzania Development Vision 2025
TeSWs	Tanzania Electronic Single Window System
TRA	Tanzania Revenue Authority
TTCL	Tanzania Telecommunications Corporation Limited
TZCERT	Tanzania Computer Emergence Response Team
UN	United Nations
URT	United Republic of Tanzania
WAMS	Workflow Automation Management System
WAN	Wide Area Network

FOREWORD

The use of the Internet has created new opportunities for cyber criminals and those with bad intentions to seek access to our personal and Government data, steal our resources and threaten Internet dependent operations. In that regard, the Government aims to work closely with Cyber security stakeholders to enable a collaborative and coordinated approach to strengthen Government cyber security implementation. With the persistence and ingenuity of all those who would threaten us, we need to work even harder to keep pace with the threats that are raised due to the advancement of technology.

I am pleased to present the Government Cyber Security Strategy 2022, which lays out our collective plan to defend against cyber-attacks and make government MDAs more secure. The Government ICT service platforms, data, and key infrastructures will be better protected from present and future security threats, thanks to the measures put in place according to this Strategy, which will be of use to all public institutions and stakeholders. We have a responsibility to ensure that the government implements a national Cyber Security Strategy that is comprehensive and effective. This strategy has been established to protect the many government agencies and platforms that are responsible for delivering vital services to the public, facilitating our digital government and safeguarding our Government's cybersecurity interests.

Thus, I would like to express my deepest gratitude and recognize the stakeholders who have exhibited and continue to demonstrate genuine solidarity and extraordinary commitment in the formulation of this Cyber Security Strategy 2022. On behalf of PO-PSMGG, I would like to express my gratitude and appreciation to everyone who has provided invaluable assistance in the development of the Government Cyber Security Strategy 2022.

Hon. Jenista J. Mhagama (MB)

Minister of State, President's Office, Public Service Management and Good Governance

PREFACE

Creating a stronger, better-defended e-Government is the foundation for delivering Government services that are resilient to cyber threats. In 2016, the Government of Tanzania launched the first Government Cyber Security Strategy which lay the foundation for subsequent Government cyber security initiatives. Under the e-Government strategy, the government has continued to utilize and deploy various digital technologies in order to modernize its business processes and improve service delivery in various sectors of the economy.

The government also recognizes that as public services become increasingly digitalized, they become more vulnerable to cyber-attacks. Thus, as the government continues to push for digitalization in the public sector, it improves cyber security protection levels in order to safeguard government systems, data, and vital infrastructure against emerging cyberspace security threats and malicious actors.

This cyber security Strategy 2022 marks the next step in the Government's journey to becoming a more cyber resilient institution. As the cyber environment evolves rapidly, the government is determined to develop new capabilities to protect data, systems, and infrastructure by strengthening support for cyber security innovation; training government ICT cyber security professionals; and raising cyber security awareness among all stakeholders.

As Government, we have made a great deal of progress in recent years, and the Cyber Security Strategy 2022 has taken a more proactive stance to address threats, broadens the scope of cyber protection and develop a deeper collaboration and coordination with all Government stakeholders to adapt to the changes in cyber operating environment. The Strategy seeks to build on the progress made by the existing e-Government policies, laws, regulations, strategies, guidelines and standards which will advance the development of cyber norms and affirm the applicability of cyber security visions.

Due to the serious nature of cyber threats we are facing, the Government has mandated that all public institutions take proactive measures to secure their ICT systems, data, and infrastructure in accordance with the objective and targets outlined in this strategy. PO PSMGG will keep an eye on how well it is put into practice and periodically revise it in light of new technologies and the growing complexity of government cyber security threats to make the public sector more resistant to cyberattacks.

Dr. Laurean J. P. Ndumbaro
Permanent Secretary
President's Office, Public Service Management and Good Governance

EXECUTIVE SUMMARY

BACKGROUND

Information and Communication Technologies have undergone significant evolutions over the last two decades and are now an integral part of every aspect of our lives. Enabling the delivery of essential Government services (such as electricity, finance, transportation, water, and healthcare) through cyberspace introduces new threats and opens the door to potential cyber incidents. The expansion of Internet services, beyond computers and mobile phones, into smart devices and systems has also extended threats of exploitation to a wider domain digital ecosystem around the world. Furthermore, since most of the Government services are now reliant on the Internet, the growing number of Internet-based services further complicates the risk of cyber threats.

This Government Cyber Security Strategy 2022 has been developed using broad engagements of stakeholders. The Strategy has been built on the achievements, objectives and strategies placed in the last five years. The Strategy facilitates the Government's journey of becoming a cyber-resilient Government in cyberspace. The Government of Tanzania intends to roll out cyber security awareness campaigns and encourage public institutions to adopt cyber security best practices; invest in developing Government cyber security professionals; strengthen support for innovation in cyber security; and assist individuals in pursuing a career in cyber security and digital forensics in order for it to adapt to the rapidly evolving cyber services landscape. Compared to the cyber security Strategy 2016, the cyber security Strategy 2022 ensures a disciplined approach and navigation to the constant changes taking place in the cyber sphere, takes a more proactive stance to address threats, broadens the scope of protection and seeks to develop deeper collaboration and coordination with institutional stakeholders.

This Cyber Security Strategy sets out how the Tanzanian Government will establish itself as a democratic and responsible cyber resilient Government in a world fundamentally shaped by technology. Threat actors in the cyber environment are becoming more sophisticated and taking advantage of increasingly ubiquitous connectivity to launch more cyber- attacks. The Government of Tanzania thus reviewed its cyber security strategy, which was first launched back in 2016. This Government Cyber Security Strategy 2022 outlines strategic goals and approach to adapt a rapidly evolving technological environment in the public sector.

THE CYBER SECURITY STRATEGY 2016

Assessment conducted to the performance based on implementations of four Key Result Areas (KRAs) as stipulated in the Government Cyber Security Strategy 2016, and the way forward to incorporate into the new Strategy. The Key Result Areas that were assessed to determine the achieved performance and challenges were:

I. Cybersecurity Threat Awareness and Response;

II. Knowledge, Skills and Innovation on Cyber Security;

III. Secure and Resilient Cyber Environment;

IV. Strengthen Legal and Regulatory Framework.

CYBER SECURITY STRATEGY 2022 -2027

The development of Cyber Security Strategy 2022 has involved the performance assessment of implementations of the four (4) Key Result Areas (KRAs) of the Government Cyber Security Strategy 2016 - 2021.

The assessment of the Key Result Areas identified some issues that contributed to the challenges encountered during the implementation of the Government Cyber Security Strategy 2016. The issues have been factored as the critical inputs into the new Strategy 2022, and include:

I. Increase in cyber-attacks on Government systems;
II. Limited bandwidth and coverage of GovNet infrastructure;
III. Inadequate Government Data center resources;
IV. Inadequate skills and mechanism for detecting, managing, and responding to cyber incidents;
V. Lack of readiness among public institutions to use Government approved hosting environment; l
VI. Limited budget for Cyber Security aspects; and
VII. Most public institutions lack a cyber security unit or personnel.

The Government has a crucial role to play in developing a cyber resilience strategy that is built on a comprehensive, consistent and flexible cybersecurity framework across the entire public sector. The Government Cyber Security Strategy 2022 has been developed with five objectives that set the dimensions of Government cyber resilience and provide a consistent framework and common themes that can be used across the whole public sector. The five objectives include:

1. Research and Development in Cyber security Technologies improved
2. Government ICT Infrastructure and e-Services Protection Enhanced
3. Cyber Security and Resilience of ICT systems Strengthened
4. Cyber security Skills, Knowledge and Awareness improved and
5. Management of Cyber security risks and incidents enhanced

The objective is to link the Government Cyber Security Strategy 2022 with the National Cyber Security Strategy 2018, the e-Government Strategy 2022, the National Cyber Security Communication Strategy 2021, and other sector-specific plans that encompass the Government's efforts to develop a stronger, more secure, resilient, synergistic, and holistic e-Service ecosystem, as Tanzania strives for a Digital Government that consistently delivers quality public services public services anywhere and anytime. Accordingly, the strategy makes it easier for all public institutions and stakeholders to have access to credible cyber security advice and support, while also strengthening the protection of important government systems, data, and infrastructure.

1. INTRODUCTION

1.1 Overview

Information and communication technologies (ICT) have evolved over the last two decades and are now integrated into virtually every aspect of our lives. ICT, being an enabler in the delivery of essential Government services such as electricity, finance, transportation, water and healthcare, has introduced new threats and opens the door to potentially catastrophic consequences from cyber incidents. Similarly, the expansion of the Internet beyond computers and mobile phones into other cyber-physical devices and systems has also extended the threat of remote exploitation to cyber-attacks from anywhere and anytime around the world. The Government Cyber Security Strategy 2022- 2027 has been developed to protect the Government Cyber environment from those threats.

The Government Cyber Security Strategy sets out how the Tanzanian Government will establish itself as a democratic and responsible cyber resilient Government in a world fundamentally shaped by technology. Threat actors in the cyber environment are becoming more sophisticated and taking advantage of increasingly ubiquitous connectivity to launch more cyber-attacks. The Government of Tanzania thus reviewed its cyber security strategy, which was first launched back in 2016. This Government Cyber Security Strategy 2022 outlines strategic goals and approach to adapt a rapidly evolving technological environment in the public sector.

This Strategy has been developed to build on the first Government Cyber security Strategy 2016. It intends to set the stage to transition the Government from the current institutionalized silo-based cyber environment into collaborated secured cyber environment that promotes efficient and effective delivery of public services. The Strategy has been developed using broad stakeholder engagement with a large number of Government entities.

This Strategy aligns with the Government's development priorities as articulated in the National Five-Year Development Plan III (FYDP III) and the Ruling Party manifesto 2020 to encompass efforts by the Government to develop a stronger, secured, resilient, synergistic and holistic e-service ecosystem as Tanzania marches towards attaining Tanzania Government Vision 2025. It is also in line with the National Cyber Security Strategy 2018, e-Government Strategy 2022, National Cyber Security Communication Strategy 2021, and other Sector-specific Plans.

The Government Cyber Security Strategy 2022 provides a framework to execute cyber security responsibilities during the next five years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities; countering malicious actors in cyberspace; responding to incidents; and making the Government cyber ecosystem more secure and resilient.

1.2 Mandate on Government Cyber security management

I. President's Office – Public Service Management and Good Governance

a. The mandate of the President's Office, Public Service Management and Good Governance (PO PSMGG) in relation to the Strategy is to develop, monitor, evaluate and review its implementation. It is also responsible for creating awareness on cyber security threats and provide policy advices on all ICT security matters in the public sector.

II. The e-Government Authority (e-GA)

b. The responsibility of the e-Government Authority (e-GA) in relation to the Strategy is to: develop a mechanism for enforcement; to coordinate its implementation; and provide cyber security technical guidelines, standards, training and awareness to all public institutions.

III. Public Institutions

c. The responsibility of Public Institutions is to implement the Strategy and ensures that they comply with the Strategy.

1.3 Purpose of the Strategy

The purpose of the Government Cyber security Strategy 2022 is to provide a broad cyber security framework to Public Institutions in order to efficiently and effectively execute cyber security responsibilities during the next five (5) years. The ultimate goal is to minimize cyber vulnerabilities, promptly respond to cyber incidents and make the Government cyber ecosystem more secure and resilient.

1.4 Scope of the Strategy

The Strategy considers all Tanzania public institutions. It intends to assist public institutions in assessing and articulating the micro cyber security posture of their respective organizations. Public institutions are therefore having the responsibility to ensure that their functions and services are resilient to cyber risks. The Strategy also sets out the Government to continue to work collaboratively with stakeholders with appropriate information and support being shared to maintain the resilience of the Government services.

2. SITUATIONAL ANALYSIS

The Strategy considers all Tanzania public institutions. It intends to assist public institutions in assessing and articulating the micro cyber security posture of their respective organizations. Public institutions are therefore having the responsibility to ensure that their functions and services are resilient to cyber risks. The Strategy also sets out the Government to continue to work collaboratively with stakeholders with appropriate information and support being shared to maintain the resilience of the Government services.

2.1 Government Cyber Security Strategy 2016 KPA Analysis

The assessment covers the performance based on implementations of four Key Result Areas (KRAs) as stipulated in the Government Cyber Security Strategy 2016, and the way forward to incorporate into the new Strategy. The Key Result Areas that were assessed to determine the achieved performance and challenges were:

I. Cyber Security Threat Awareness and Response;
II. Knowledge, Skills and Innovation on Cyber Security;
III. Secure and Resilient Cyber Environment;
IV. Strengthen Legal and Regulatory Framework.

The accomplishments in each of the KRAs identified are described as follows:

A. Cyber Security Threat Awareness and Response

The major Government Cyber Security Strategy 2016 accomplishment with respect to cyber security Threat Awareness and Response include:

I. To fulfil the needs for citizens' awareness, the following initiatives were achieved: - 12 cyber security awareness events were conducted; 548 Government staff attended e-Government cyber security awareness programs; 1556 participants attended e-Government Conferences held in Arusha and Dodoma, on which cyber security was among the agendas that were presented; and 48 cyber security issues reported from Public Institutions were responded.
II. Transformation of the e-Government Agency into e-Government Authority in 2019, with the full department responsible for cyber security matters and compliance.

B. Knowledge, Skills and Innovation on Cyber Security

The major Government cyber security Strategy 2016 accomplishment in this area include:

I. Provision of e-Government technical training that with cyber security aspects includes: - network and security management to 240 institutions; e-services to 76 institutions; website management to 411 institutions; ICT strategic management to 150 staff; ICT infrastructure and connectivity to 173 staff; e-Government standards and guideline to 149 staff; and application systems to 783 staff.

II. Increase the number of ICT security personnel in the public service to 102 staff by 2022.

C. Secure and Resilient Cyber Environment

The major accomplishment includes:

I. Connection of 265 MDAs and LGAs to secure Virtual Private Government Communications Network (GovNet);

II. Establishment and operationalization of the Government Data-Centre (GDC) which provides secure Government cloud computing, web hosting, server colocation and other operations;

III. Provision of cyber security technical assistance and security assessments to 422 public institutions.

D. Strengthen Legal and Regulatory Framework

The major accomplishment includes:

I. The e-Government Act, 2019 and its Regulations 2020 were enacted, allowing for legal provisions for Government cyber security issues including the establishment of the Government Security Operation Centre;

II. Development of e-Government security standards and guidelines for Public Institutions; and

III. Appointment of an ICT Officer as a Cyber Security Focal Personnel in each Public Institution.

2.2 Challenges of Implementing Government Cyber Security Strategy 2016 - 2021

Despite the achievement made on the implementation of the Government Cyber security Strategy 2016, some challenges were encountered as illustrated in Table 1:

Table 1: Challenges of Implementing the Government Cyber Security Strategy 2016;

i. Inadequate budget to provide training on cyber security issues to some public institutions;

ii. Inadequate ICT Security Personnel in some public institutions to coordinate ICT security issues;

iii. Inadequate professional training on cyber security;

iv. Existence of a digital divide between rural and urban areas on matters related to cyber security;

v. GovNet is not fully operationalized to provide secure Virtual Network services in LGAs and service facilities;

vi. Some e-Government systems were implemented without effective security controls;

vii. There is uneven maturity in applying e-Government security initiatives among public institutions;

viii. Delays in enacting e-Government laws and regulations to provide legal provisions for cyber security issues; and

ix. Delay in having in place an Authority to enforce and oversee cyber security issues.

2.3 Stakeholders Analysis

Stakeholder Analysis provides inputs on the expectations of key cyber security stakeholders in the Government and identifies key issues that are critical in meeting stakeholders' expectations. Key stakeholders are categorized as follows: MDAs/RSs/LGAs, Public Institutions, Parliament, Trade Unions, Judiciary, Private Sectors, General Public, Media, Academic and Research Institutions, Regulators, Development Partners, Politicians, Investors, Financial Institutions and Government Employees as detailed in Table 2.

Table 2: Stakeholder's expectations

Stakeholder	Expectations
MDAs/RSs/LGAs/Public Institutions	• Security and confidentiality in the provision of e-Government services • Creating a secure enabling environment for the promotion of e-Government • Value for money and security compliance in all e-Government operations • Timely provision of accurate information for decision making.
Financial Institutions & Private Sectors	• Security, transparency and active engagement in Government e-services • Professionalism and integrity in dealing with Cybersecurity threats • Consistency and timely response to Cybersecurity queries and inquiries
Parliament/ Politicians	• Expanded coverage of secure e-Government services • Secure and trusted e-Government services for their voters • Available, quality, affordable and reliable e-Government services from Service Providers • Accurate information and knowledge
Trade Unions	• Security, transparency and active engagement in Government e-services • Professionalism and integrity in dealing with Cybersecurity threats • Consistency and timely response to Cybersecurity queries and inquiries
Citizens	• Secure, Trusted, Fair, affordable prices/charges of e-Government services • Confidentiality, Quality and reliable e-Government services from service providers • Safe, quality and environmentally friendly e-Government service delivery infrastructure.
Media & Non-State Actors	• Timely dissemination of accurate information • Access to information of public interest • Openness and cooperation in issues of national/public interest • Active participation in the e-Government security processes to enhance knowledge
Academic and Research Institutions	• Trusted, correct and accurate data • Partnership in research and use of knowledge from findings on Cybersecurity • Partnership in research and use of their research knowledge/findings on Cybersecurity
Development Partners	• Trusted and secure e-Government services • Transparency and active engagement Cybersecurity issues • Professionalism and integrity in dealing with Cybersecurity threats • Consistency and timely response Cybersecurity queries and inquiries
Investors	• Fair and reliable e-Government processes. • Timely decision-making on e-Government security matters • Trusted, secure, conducive legal and business environment in free environment from cyber threats. • Transparency, credibility, and consistency in cyber security issues

Government Employees	• Transparent, effective and efficient performance of e-Government services • Secure and timely sharing of information • Confidentiality, accessible and affordable e-Government services • Secure and conducive working environment • Enhanced ICT Security capacity building to staff.
Suppliers and Service providers	• Trusted and secure e-Government services • Transparency and active engagement Cybersecurity issues • Professionalism and integrity in dealing with Cybersecurity threats • Consistency and timely response to Cybersecurity queries and inquiries

2.4 Sector Development Frameworks Analysis

The specific subjects covered under this analysis are based on evaluations of different National Development Frameworks, namely:

I. National ICT Policy (NICTP) 2016

The National ICT Policy, 2016 highlighted the need to have a secure environment that builds safety, confidence and trust during the usage of ICT services and products as well as strengthens quality controls and standards in the ICT industry. The Government Cyber Security Strategy 2022 -2027 will contribute on the achievement of the National ICT Policy 2016 -2021 by ensuring the performance of various ICT security operations by public institutions to enhance their ICT security posture and bring the required confidentiality, integrity and availability of Government data and services. Further, the Strategy will emphasize on creation and usage of ICT security Standards and Guidelines across public institutions for proper coordination of various ICT security initiatives in public institutions.

II. e-Government Strategy 2022

The e-Government Strategy 2022 - 2027, elaborated on the seven strategic pillars that will pave the way and shape its implementation over the next five years. The pillars are connected Government, institutional collaboration and coordination, e-Government Services, e-Government research and innovations, e-Government cyber security ecosystem, e-Government human capital development, e-Government policies, legal and institutional framework.

This Strategy will contribute on the achievement of the e-Government Strategy 2022 strategic pillars by: enforcement of ICT security standards and guidelines to ensure coordinated efforts on various ICT security across Government in areas such as systems development, systems integration as well as during development of institutional ICT security frameworks. The Strategy will also enforce ICT security operations, ICT security human capital development and conducting ICT security awareness programs to build and entrusted cyber security ecosystem within the Government.

III. National Cyber Security Communication Strategy 2021

The national Cyber Security Communication Strategy 2021 highlighted its major objectives to enhance awareness and impart knowledge on Cyber Security Policies, Strategies, Laws,

Regulations and Guidelines. It also demonstrates areas for improving customer service on cybercrime issues among stakeholders involved, and how to create awareness to the general public on the mandate of different key stakeholders in handling cybercrime incidents.

The Government Cyber Security Strategy 2022 will contribute to the achievements of the National Cyber Security Communication Strategy by providing cyber security training and awareness sessions to public institutions' management, technical and other Government employees.

IV. National Cyber Security Strategy 2018

National Cyber Security Strategy 2018 is built on five guiding principles, namely: Public-Private Partnerships; Ubiquitous threats; Risk based Management; Capacity Building and Awareness for all; and Regional and International collaboration. In line with these principles, the National Cyber Security Strategy 2018 outlined five strategic goals including Protection of Critical Information Infrastructure; Increase Cyber security technical capabilities and awareness; Promote collaboration, coordination 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 secure cyberspace in Tanzania.

The Government Cyber Security Strategy 2022 will contribute to the achieving the National Cyber security Strategy 2018 by: promoting Research and Innovations in cyber security; ensuring cyber security Human Capital Development; enhancing Collaboration and Coordination among Government institutions and stakeholders in protecting Cyberspace; Improving the protection of Data, Systems and Infrastructure.

2.4 SWOC Analysis

A. Strengths

b) In terms of the legal environment, the presence of the e-Government Act of 2019 and its Regulations (2020) and e-Government Strategies, Standards and Guidelines for Public Institutions to use and comply in shaping their e-Government security initiatives.

c) On the Governance: - the presence of well-established e-Government security structures with an average number of human resources to facilitate e-Government implementation; the existence of TZ-CERT; the existence of e-Government security operation Center (eGSOC); the existence of database for single point of contact (SPOC) for public institutions on ICT security related matters; and the establishment of e-Government Authority from e-Government Agency in 2019.

d) With regard to application systems, major mission-critical application systems have been implemented in a secured environment to cater for the crosscutting business operations with the majority of these systems being home-grown. Key areas where

systems have been implemented include the Population registry, Land Management registry, Collaboration Systems, and Human Capital and Financial systems.

e) In terms of e-Government infrastructure: - the development of the Government e-Payment Gateway (GePG) that facilitates revenue collection; the deployment of the Government Network (GovNet) that allows public institutions to communicate securely; and the implementation of Government Data-centres that provide a conducive hosting environment for hosting Government systems.

f) In terms of e-Services: - over 500 websites and portals have been implemented with e-security consideration to support e-Government services initiatives; presence of a variety of e-services and mobile services that are offered by different public institutions through different secured channels; and the securely Government Portal as a one stop service centre for Government services and information.

B. Weaknesses

a) In terms of Governance; the weakness observed include: limited awareness of existing e-Government security laws, regulations as well as standards and guidelines among public servants and law enforcers; and a lack of some essential security standards and guidelines that need to be developed and implemented.

b) In terms of Human resources; - lack of adequate expertise in ICT Security personnel in some specialized areas, which poses risks to sustainability of some cyber security initiatives; inadequate awareness of Cyber security among Government employees and citizens at large; and lack of highly trained cyber security personnel in the Government which leads to inadequate cyber security skills posing the risk of cyber-attacks.

c) In terms of application systems, there is relatively low research and innovation in the area of cyber security and low-security maturity level among public institutions.

d) On the e-Government infrastructure, weaknesses include: insufficient computing and storage capacity at the Government Data-centre to support storage securely and access to Government applications; and inadequate cyber security tools to support combating cyber security events.

e) The e-services weaknesses include: - Insufficient customer support systems (Helpdesks) for handling Government cyber security-related complaints; and a lack of adequate skills and mechanisms for detecting, managing, and responding to cyber incidents.

C. Opportunities

a) In terms of policy, laws and regulations, the opportunities are: - the presence of the National Cybersecurity Policy 2018 which supports the implementation of Government cybersecurity; the Electronic Transactions Act of 2015 and the Cyber Crime Act of 2015 which provides legal provision for e-Government transactions and e-Government

security; the existence of political will from the top leadership of the Government in supporting of cybersecurity agenda.

b) Opportunities related to ICT Governance are: the presence of a skilled ICT security workforce who can be employed by the Government; and the existence of the Tanzania Computer Emergency Response Team (TZCERT) that oversees, among other functions, the implementation of Cyber security issues related to e-Government.

c) In terms of application systems, opportunities include the existing political willingness to innovate, build and adopt secure home-grown e-Government systems in the provision and delivery of Government services.

d) Opportunities related to e-Government Infrastructure include: - the availability of the ICT Broadband backbone in the country that supports the implementation of secure Government infrastructure and the presence of the National Data-centre which has dedicated 25% of its capacity for securely hosting and protecting e-Government e-services.

e) e-Services opportunities include the existence of security consciousness among young and technically savvy users representing a ready market for e-services.

D. Challenges

a) Challenges related to policy, laws and regulations include lack of a comprehensive legal framework for cooperation with external partners in Cyber Security matters.

b) In terms of application systems, existing challenges are: different pace in establishing and adopting e-Government initiatives among public institutions; inadequate skills in public institutions to cope with emerging technologies; lack of sustainability of some e-Government initiatives especially those that are donor funded after the expiration of the funding period; and the existence of malicious Cyber Security software/hardware tools.

c) On the e-Government infrastructure, existing challenges include: limited coverage of the National ICT infrastructure backbone in the Local Government Authorities to facilitate e-Government Services and the high costs of hosting e-Government services in the National Data-centre.

d) Challenges related to e-Services include a high level of computer illiteracy, including cyber security-related issues in the society, and reliance on external experts and technology solutions in the area of Cyber security.

2.6 Recent e-Government Cyber Security Related Initiatives

The following are Government initiatives in the area of ICT security initiatives:

I. e-Government Research, Innovation and Development Centre (e-GovRIDC)

The e-Government Research, Innovation and Development Centre (e-GovRIDC), under e-Government Authority, has been established to oversee the management and monitoringof research and innovations in the area of e-Government including e-security. It is expected that the centre will coordinate researches and innovations that will support the Government strategy to deal with Cyber security issues.

II. Digital Tanzania Programme (DTP)

Digital Tanzania Programme is a World Bank-funded project whose development objective is to increase access to high-quality internet services for Government and citizens, and to improve the Government's capacity to deliver digital public services. The DTP initiatives that cybersecurity strategy 2022 will take advantage include: ICT regulatory scan and review; Enhancement of Government ICT Connectivity; development of digital services and productivity platforms; enhancement of Data-centre Infrastructure; and Government ICT cadre training programme and Citizen Digital Literacy.

2.7 Critical Issues

Critical issues that were encountered during the implementation of the Government Cyber Security Strategy 2016, which need to be addressed by the new Government Cyber security Strategy 2022 include:

I. Increased cyber-attacks incidents on the e-Government systems;

II. Inadequate skills and mechanism for detecting, managing and responding to cyber incidents;

III. Lack of readiness among public institutions to use Government approved hosting environment;

IV. Insufficient budget for Cyber Security initiatives; and

V. Inadequate of Cyber Security unit/personnel in most public institutions

3. THE GOVERNMENT CYBER SECURITY STRATEGY 2022-2027

3.1 Advances in Cyber Security Technologies

The world is experiencing an unprecedented advancement of cyber security technologies, accompanied by an equally rapid surge in persistent and sophisticated cyber hackers. Thus, e-Government stakeholders, especially academic and research institutions, need engage in Cyber security research, innovation, and development in order to address emerging cyber security threats that may adversely impact current e-Government initiatives.

Citizens are increasingly demanding that most major government functions in public institutions be delivered online. As a result of the global expansion in e-services, there has also been an increase in cyber-attacks. Importantly, the public sector remains vulnerable to cyber assaults, especially ransomware, which has gotten more lethal and destructive in recent years.

Tanzania has made remarkable progress in digitalizing government services, including the processing, sharing, and usage of electronic data to make informed decisions based on data analysis. The outcome is a noticeable improvement in delivery of services to companies and countries. This sharp increase in digitalization raises the stakes for the security of information and communication technology systems and infrastructure.

Public Institutions are responsible and accountable for managing their own cyber security risks needed to build cyber resilience on Government systems and by ensuring they can respond to numerous cyber events. Cyber security risk management is a top priority; therefore, these institutions should establish the appropriate management structures, raise cyber security awareness, and implement cyber security solutions based on best practices.

In the strategy, the Government takes the initiative in ensuring e-services are delivered to the citizens through public institutions with maximum security on information from the point of creation, during transit, where the information used and where the information is finally stored. The strategy emphasizes the need to protect and govern the data, as well as the service delivery platforms and infrastructure.

This Chapter presents the entire Strategy for 2022 – 2027 in terms of (objectives and targets) that are envisaged to be implemented and realized in five years period. The chapter shows also how the various strategic interventions to be undertaken during the five years of the strategic implementation that will lead to achievement of the Development Objective.

3.2 Vision

Our vision is to ensure a secure and resilient cyberspace for efficient and effective delivery of public services.

3.3 Mission

Our mission is to protect Government ICT platforms and safeguarding the confidentiality, integrity and availability of critical information infrastructures from cyber threats and vulnerabilities, enabling seamless and secure implementation of e-Government initiatives.

3.4 Cyber Security Strategic Objectives

The e-Government Cybersecurity Strategy 2022 is underpinned by five (5) objectives. These objectives establish the scope of what must be considered in establishing cyber-resilience in the public sector. Among the five aims are the following:

1. Research and Development in Cyber Security Improved.
2. Government ICT Infrastructure and e-Services Protection Enhanced.
3. Cyber Security and Resilience of ICT Systems Strengthened.
4. Cyber Security Skills, Knowledge and Awareness Improved.
5. Management of Cyber Security Risks and Incidents Enhanced.

3.5 Cyber Security Strategic Outcome areas

3.5.1 Objective A: Research and Development in Cyber Security Technologies Improved

Rationale

The threats and risks in the cyber space are becoming more sophisticated as technology develops. Research, Innovation, and Development (RI&D) will therefore be an integral component in the war against future cyberattacks. This Strategy aims to increase cooperation with the private sector and collaboration with other nations on cybersecurity issues. This will help to facilitate combating the borderless nature of cyber threats related to Government services. With this Strategy the Government will be establishing appropriate instruments for collaboration and the exchange of information. These instruments will facilitate procedures for the access to and transmission of information on the area of concern.

Moreover, to strengthen its cyber resilience and proactively tackle the critical cyber security challenges, the Government relies on international partners, higher education institutions, and the private sector.

Strategy:

i. Fostering Research, and Innovation in cyber security including related emerging technologies;

ii. Promote information sharing and collaboration on cyber security;

Targets:

i. Five (5) collaborations with research institutions facilitated by June 2027;

ii. e-Government Research and Innovation Centre on cyber security matters capacitated by June 2027;

iii. Three (3) Government cyber security projects evaluated, monitored and approved by June 2027;

iv. Three (3) Collaborations on cyber security with private sectors and international partners facilitated by June 2027;

v. Five (5) cyber security skills competition projects facilitated by June 2027;and

vi. Five (5) Government ICT security forums with Public Institutions' heads of ICT conducted by June 2027

3.5.2 Objective B: Government ICT Infrastructure and e Services Protection Enhanced

Rationale

Almost every aspect of life today is affected by digital technologies. Broadband networks and wireless signals enable modern society to conduct business and provide Government services in a safe and secure manner. Cybersecurity is essential to the sustainability of growing economies and the protection of Government services is a major component of the strategy. In response to the increasing demand for e-services delivered by the Government to citizens, the internet has become more accessible to devices, which has led to an expansion of cyber-attacks. Thus, the Government must take the initiative to ensure that e-services are provided to citizens in a secure manner by public institutions. Cyber-protection should be supported through the aforementioned rewards program and through the provision of tools to check system security status.

Cybercriminals use sophisticated and malicious tactics to undermine critical infrastructure, steal intellectual property and innovation and engage in espionage. Public institutions are also increasingly utilizing IP-based physical security systems, such as video surveillance, fingerprint scanners, access control cards, etc., which presents cybercriminals with new attack points. It is imperative that Government critical infrastructure adheres to the National Critical Information Infrastructure Guidelines to provide essential services.

Strategy:

i. Strengthening security of e-Government services;

ii. Strengthening security on implementation of e-Government infrastructure.

Targets:

i. Government's Critical Information Infrastructure (CII) guidelines Develop and operationalize by June 2023;

ii. Government Public Key Infrastructure (PKI) developed and operationalized by June 2027;

iii. 660 Public institutions' sites connected to Government Network (GovNet) by June 2027; and

iv. 90% Public institutions systems exchange data through GovESB by June 2027.

3.5.3 Objective C: Cyber Security and Resilience of ICT systems Strengthened

Rationale

Cyber incidents can be prevented by maintaining an ethical culture within public institutions. In accordance with the e-Government Strategy 2022, the cyber security strategy 2022 creates a dedicated e-Government Cyber security ecosystem and lays the foundation for the development of critical infrastructure Cyber security guidelines.

Throughout the development life cycle of critical systems, public institutions should ensure that system developers have security experts embedded within their teams to provide continuous security advice. Using a 'secure by design' framework, public institutions can ensure that all e-services are planned, procured, designed, developed, operated, modified and decommissioned securely, taking into account e-Government standards and guidelines.

By implementing this strategy, the Government aims to improve the resilience and security of the ICT systems used by the public sector, thereby improving the security of data and the delivery of services to citizens. Public institutions must implement standards to support continuity of ICT systems, recovery from disasters, and business continuity to achieve sufficient cyber resilience.

Strategy:

i. Enhance confidentiality, integrity, availability, and reliability of e- Government systems; and

ii. Strengthen e-Government cyber security operations.

Targets:

i. Government electronic Data Management Guideline developed and operationalized by June 2027

ii. e-Government Capability Maturity Framework developed and operationalized by June 2023;

iii. Baseline ICT security standard as per Institution's ICT Maturity levels established and operationalized by June 2025;

iv. e-Government Security Operations Center capacitated by June 2025;

v. 100% Public institutions' critical Information Systems hosted on Government approved hosting environment by June 2025;

vi. Disaster Recovery Plan for all Government's critical systems developed, implemented

and tested by June 2024;and

vii. e-Government security operations Guidelines developed and operationalized by June 2023

3.5.4 Objective D: Cyber security skills, knowledge and awareness Improved

Rationale

It is imperative for public institutions to develop a well-trained workforce with sufficient cyber security knowledge, in accordance with their roles and responsibilities. As a result of this workforce, incidents will be managed and the organization will be protected. Additionally, cyber security threats need to be proactively addressed through training, conferences, and workshops. In order to achieve the Strategy's goals, Government employees will be empowered to proactively engage in institutional cyber security risk management.

Institutions should work to increase awareness of cyber security threats, risks, and the necessary measures of protection across the organization. Among these measures are reinforcing the expectations of public servants and embedding cyber security awareness within public service values. To maintain information security, employees must be aware of their responsibilities. This is why their support is necessary, and what happens if cyber security policies and procedures are not followed. A comprehensive and continuously evolving employee awareness program should be offered to new employees within an organization. The increased use of social media by youth in Tanzania necessitates the provision of cyber security awareness training to academic institutions and secondary schools.

Cyber security best practices can be promoted, cyber security threats can be reduced, and the resilience of Government systems and infrastructure can be increased by increasing capacity building and awareness of cyber security. In accordance with the e-Government standards, public institutions are required to develop a range of cyber security skills and knowledge, and ensure that their personnel are inclusive and diverse in order to comply with all requirements related to cyber security. A secure e-Government service is more likely to be adopted if Government employees are generally aware of cyber security issues. This will ensure that all employees are better protected and the institution will be more secure.

Strategy:

i. Promote Cyber security awareness

ii. Strengthen capacity for ICT security personnel

Targets:

i. Government cyber security awareness program developed by June 2024;

ii. Security awareness programs for 100% of Public institutions conducted by June 2027;

iii. Cyber security syllabus to Secondary schools developed and operationalized by June 2027;

iv. One Government platform for provision of cyber security awareness and knowledge testing established and operationalized by June 2025;

v. 15 training programs for ICT security personnel developed and operationalized by June 2027;

vi. Cyber security capacity building to increase professional competencies to 500 ICT Security Personnel conducted by June 2027; and

vii. Cyber security awareness to 90% of Higher Education conducted by June 2027.

3.5.5 Objective E: Management of Cyber security risks and incidents Enhanced

Rationale

The effective management of the risks derived from cyberspace must be built on a sound culture of cyber security in all public institutions. To ensure that the information, systems, and services of the Government are protected, it is essential that Government officials understand the risks and are familiar with the tools available for protecting them. Whether it is infrastructure, information and communications technology systems or data, public institutions should have visibility into and an understanding of the assets they own and operate, as well as the threats that may occur to them. This includes incidents of identity theft and identify fraud. Each public institution is responsible for identifying, assessing, understanding, and managing risks.

On the basis of institutional risk management, all public institutions should be able to detect cyber security events across organizations. By doing so, we will be able to mitigate the risks before they negatively impact Government services. In order for public institutions to monitor and mitigate cybersecurity risks, they must develop mechanisms for assessing risks. In addition, they must develop governance arrangements that will allow them to drive the necessary improvements. Institutional Accounting Officers should be responsible for their organization's risk and maintain oversight and responsibility to ensure that cyber security risks are identified and managed. Information about cyber security risks and incidents should be shared among public institutions, and incident management should be handled by a centralized infrastructure. This will help to prevent incident spread and allow reporting of incidents.

There is the possibility that third parties may provide systems, products, and services that may pose a risk. This strategy encourages public institutions to implement an active and automated asset management process. As a result, they will be able to determine what hardware, software, and systems they own and operate and how to manage potential risks. The public sector should also take steps to better understand its dependence on suppliers. As part of their integration into Government systems, they should ensure that their products and services take full account of the impact they are projected to have on security and resilience. It is pertinent to recognize

that new technologies, such as the internet of things (IoT) pose risks, as attackers may exploit these technologies to their advantage.

As a result of the implementation of this Strategy, public institutions will be able to demonstrate that they have appropriately considered cyber risks and implemented appropriate responses.

Strategy:

i. Improving ICT security governance;

ii. Developing ICT Security operations and implementation standards and guidelines

iii. Strengthening of ICT systems monitoring against cyber threats

Targets:

i. Operationalization of ICT Security standards and guidelines in 90% of public institutions quarterly facilitated by June 2024;

ii. 100% of Public Institutions Compliance on ICT Security operations standards and guidelines monitored by June 2027;

iii. 90% of Public Institution's Incident Response Management plans developed by June 2024;

iv. Cyber security incident registry developed and operationalized by June 2024;

v. Database of Government single point of contact maintained and managed by June 2027;

vi. Institutional ICT Risk Management Plan established and operationalized by June 2024;

vii. 100% Compliance and audit programs to mitigate risks to critical e-services in public institutions conducted yearly;

viii. 95% of Annual reported security incidents responded by June 2027;

ix. 95% of Public institutions' critical systems monitored against cyber-attacks by June 2024;

x. 95% of Public institutions' ICT Security Policy developed and operationalized by June 2027.

xi. Once-Only Principle for Government services implemented and operationalized by June 2024

4. RESULTS FRAMEWORK

This chapter outlines how the intended results as well as the benefits of implementing interventions under the Government Cyber Security Strategy 2022. Cyber security is both an imperative and an opportunity. In this context the results framework presented is essentially a management tool intended to guide the Government in pursuit of its strategic vision and mission in Cyber Security Strategy. It also provides the Results Framework Matrix and the Monitoring Plan.

4.1 Development Objective

The overriding developmental objective represents the highest level of result envisioned by the Government and will be achieved through specific objectives that are: -

(a) Research and Development in Cyber Security Improved;

(b) Government ICT Infrastructure and E-Services protection Enhanced ;

(c) Security and Resilience of ICT Systems Enhanced;

(d) Cyber Security Skills, Knowledge and Awareness improved;

(e) Management of Cyber Security Risks and Incidents Enhanced;

4.2 Beneficiaries of the Cyber Security Strategy

The Cyber Security Strategy comprises direct and indirect beneficiaries:

Direct beneficiaries of the services offered through this Strategy are:

- Ministries and Independent Departments
- Executive Agencies
- Regional Secretaries and Local Government
- Public Institutions

Indirect Beneficiaries are:

- Stakeholders
- Citizens

4.3 Results Framework Matrix

The Results Framework Matrix contains Government Cyber Security Objective, Strategy Target and Key Performance Indicators. The matrix envisions how the Development Objective will be achieved and how the results will be measured. The indicators in the matrix will be used to track progress towards achievement of the Intermediate Outcomes and Objectives. The Results Framework Matrix is as detailed in Table 3.

Table 3: Results Framework Matrix

Objective	Strategy	Target	Outcome Indicators
Research and Development in Cyber Security Improved	Fostering Research, and Innovation in cyber security including related emerging technologies; Promote information sharing and collaboration on cyber security;	Five (5) collaborations with research institutions facilitated by June 2027; e-Government Research and Innovation Centre on cyber security matters capacitated by June 2027; Three (3) Government cyber security projects evaluated, monitored and approved by June 2027; Three (3) Collaborations on cyber security with private sectors and international partners facilitated by June 2027; Five (5) cyber security skills competition projects facilitated by June 2027; Five (5) Government ICT security forums with Public Institutions' heads of ICT conducted by June 2027.	Percentage level of collaboration between public institutions and private sectors Ratio home-grown cyber security solution innovated Level of Percentage in cyber security projects evaluated and approved Percentage of cyber security forums conducted
Government ICT Infrastructure and e-Services protection Enhanced	Strengthening security of e-Government services; Strengthening security on implementation of e-Government infrastructure.	Develop and operationalize Government's Critical Information Infrastructure (CII) guidelines by June 2023; Government Public Key Infrastructure (PKI) developed and operationalized by June 2027; 660 Public institutions' sites connected to Government Network (GovNet) by June 2027; 90% Public institutions systems exchange data through GovESB by June 2027.	Percentage of public institutions operationalizing the Government's Critical Information Infrastructure (CII) guidelines Percentage of Government critical systems that utilize Public Key Infrastructure (PKI) Percentage of public institutions connected and utilizing GovNet Percentage of Government systems exchanging data through GovESB

Security and resilience of ICT systems improved	Enhance confidentiality, integrity, availability, and reliability of e- Government systems; Strengthen e-Government cyber security operations.	Government electronic Data Management Guideline developed and operationalized by June 2027 e-Government Capability Maturity Framework developed and operationalized by June 2023; Baseline ICT security standard as per Institution's ICT Maturity levels established and operationalized by June 2025; e-Government Security Operations Center strengthened by June 2025; 100% Public institutions' critical Information Systems hosted on Government approved hosting environment by June 2025; Disaster Recovery Plan for all Government's critical systems developed, implemented and tested by June 2024; e-Government security operations Guidelines developed and operationalized by June 2023.	Percentage of public institutions operationalizing the Government electronic Data Management Guideline Percentage of public institutions operationalizing the -Government Capability Maturity Framework and corresponding Baseline ICT security standard Percentage of Government critical information systems hosted in approved hosting environment Percentage of Government critical information systems with tested disaster recovery plans
Cyber security skills, knowledge and awareness improved	Promote Cyber security awareness to Government Employees; Strengthen capacity for ICT security personnel; Promote cyber security awareness to universities and secondary school students;	Government cyber security awareness program developed by June 2024; Public institutions to conduct security awareness to its employees at least annually by June 2024; Cyber security syllabus to Secondary schools developed and operationalized by June 2027; Government platform for provision of cyber security awareness and knowledge testing established and operationalized by June 2025; Fifteen (15) training programs for ICT security personnel developed and operationalized by June 2027; Cyber security capacity building to increase professional competencies to 500 ICT Security Personnel conducted by June 2027; Cyber security awareness across universities conducted by June 2027	Percentage of Government cyber security awareness programs conducted Level of cyber security awareness to Government employees Percentage of certified professional cyber security personnel in public institutions Percentage of higher learning institutions that have included cyber security awareness and skills development into their curricula

Management of Cyber Security Risks and Incidents Enhanced	Improving ICT security governance; Developing ICT Security operations and implementation standards and guidelines Strengthening of ICT systems monitoring against cyber threats	Operationalization of ICT Security operation standards and guidelines in public institutions quarterly facilitated by June 2024; Compliance on ICT Security operations standards and guidelines quarterly monitored by June 2027; Incident Response Management plans by Public Institutions developed by June 2024; Cyber security incident registry developed and operationalized by June 2024; Database of Government single point of contact maintained and managed by June 2027; Institutional ICT Risk Management Plan established and operationalized by June 2024 Compliance and audit programs to mitigate risks to key e-services in public institutions conducted yearly; 95% of reported security incidents responded by June 2027; 95% of Public institutions' critical systems monitored against cyber-attacks by June 2024; 95% of Public institutions' ICT Security Policy developed and operationalized by June 2027. Once-Only Principle for Government services implemented and operationalized by June 2024	Ratio of Incidence Response Management Plan of public institutions developed and operationalized Satisfaction Level of operationalization of ICT Risk Management Plan Percentage of significant cyber security incidents responded by public institution based on their respective RTO and RPO Percentage of critical systems monitored against cyber-attacks Percentage of identity theft / identy fraud redeced in the Government Transactions

1.1 Monitoring Plan

The Monitoring Plan consists of indicators, indicator description, baseline, indicator target values, data collection, methods of analysis, indicator reporting frequencies and the officers who will be responsible for data collection, analysis and reporting as presented on Table 4.

Table 4: Monitoring Plan Matrix

INDICATOR AND INDICATOR DESCRIPTION	BASELINE	INDICATOR VALUES (%)	DATA COLLECTION AND METHODS OF ANALYSIS									FREQ. OF REPORTING	RESPONSIBILITY FOR DATA COLLECTION
	DATES	VALUES (No.)	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5	DATA SOURCE	DATA COLLECTION INSTRUMENTAND METHODS	FREQ. OF DATA COLLECTION	MEANS OF VERIFICATION		
OBJECTIVE: Research and Development in Cyber Security Improved													

Percentage of public institutions and private sectors collaborated with Government on cyber security matters. This indicator intends to show the trend of public institutions and private sectors that are collaborating with Government on cyber security matters This will be calculated by (X/(Y+Z) *100 where X= Number of public institutions and private sectors collaborated with the Government on cyber security matters, Y is the number of targeted public institution's and Z is the targeted number of private sectors	NA	NA	20	40	60	80	100	e-GA	Reports, survey	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

Proportional level of home-grown cyber security solution innovated This indicator intends to show the internal sustainability of cyber security solutions in the Government It will be calculated as X_n Where x = (Number of home-grown solutions innovated) and n=year1, year2, year 3, year4, year5	NA	NA	NA	NA	1	2	3	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

Percentage of cyber security projects evaluated and approved This indicator intends to show the trend of cyber security projects conducted, evaluated and approved per targeted time This will be calculated as (X/Y)*100 where X = number of evaluated and approved cyber security projects, and Y = Total number of targeted projects per given time	NA	NA	NA	NA	30	60	100	e-GA	Reports, survey	Annually	e-Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA
Percentage of cyber security forums conducted This indicator intends to show the internal sustainability of cyber security solutions in the Government It will be calculated as $X_n/y*100$ Where x = (Number of cyber security forums conducted) n = number of years 1, 2, 3, 4, and 5 and y = Targeted number of cyber security forums	NA	NA	20	40	60	80	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

OBJECTIVE: Government ICT Infrastructure and e-Services Protection Enhanced													
Percentage of public institutions operationalizing the Government's Critical Information Infrastructure (CII) guidelines This indicator intends to show the trend of public institutions operationalizing the Government's Critical Information Infrastructure (CII) guidelines This will be calculated by (X/Y) *100 where X= Number of public institution's operationalizing Government's Critical Information Infrastructure (CII) guidelines and Y = Total number of public institutions with Government's Critical Information Infrastructure (CII).	NA	NA	20	40	60	80	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

Percentage of Government critical systems that utilize Public Key Infrastructure (PKI) This indicator intends to show the trend of public institutions that utilize Public Key Infrastructure (PKI) This will be calculated by (X/Y) *100 where X= Number of Government critical systems utilizing PKI and Y = Total number of Government critical systems	NA	NA	20	40	60	80	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA
Percentage of public institutions connected and utilizing GovNet This indicator intends to show the trend of public institutions that are connected and utilizing GovNet This will be calculated by (X/Y) *100 where X= Number of public institutions connected to GovNet and Y = Targeted number of public institutions to be connected to GovNet	NA	NA	NA	NA	NA	NA	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

Percentage of Government systems exchanging data through GovESB This indicator intends to show the trend of Government systems to exchange data via GovESB This will be calculated by (X/Y) *100 where X= Number of Government systems exchanging data via GovESB and Y = Targeted number of Government systems that requires integration	NA	NA	NA	NA	NA	NA	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA
OBJECTIVE: Security and Resilience of ICT systems Enhanced													

Percentage of public institutions operationalizing the Government electronic Data Management Guideline This indicator intends to show the trend of public institutions that operationalize Government electronic Data Management Guideline This will be calculated by (X/Y) *100 where X= Number of public institutions that operationalized Government electronic Data Management Guideline and Y = Total number of public institutions	NA	NA	NA	NA	NA	80	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

Percentage of public institutions operationalizing the Government Capability Maturity Framework and corresponding Baseline ICT security standard This indicator intends to show the trend of public institutions that operationalize Government Capability Maturity Framework and corresponding Baseline ICT security standard This will be calculated by (X/Y) *100 where X= Number of public institutions that operationalized Government Capability Maturity Framework and corresponding Baseline ICT security standard and Y = Total number of public institutions	NA	NA	NA	NA	NA	80	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

Percentage of Government critical information systems hosted in approved hosting environment This indicator intends to measure the extent at which Government critical systems are hosted in approved hosting environment to improve Government cyber security systems ecosystem This will be calculated as: (X/Y) *100 where X = number of critical Government systems hosted in approved hosting environment and Y = Total number of critical Government systems.	NA	NA	NA	NA	100	100	100	Reports	Survey and Questionnaires	Quarterly	Reports	Annually	PO-PSMGG/e-GA

Percentage of Government critical information systems with tested disaster recovery plans This indicator intends to show the trend of public institutions whose disaster recovery plans were being periodically tested. This will be calculated by (X/Y) *100 where X= Number of critical systems whose disaster recovery plans have been tested and Y = Total number of critical systems in public institutions	NA	NA	X	X	X	X	X	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA
OBJECTIVE: Cyber Security Skills, Knowledge and Awareness Improved													

Percentage of Government cybersecurity awareness programs conducted This indicator intends to show the trend of Government cybersecurity awareness and training programs conducted to public institutions It will be calculated as (x/y)*100 where x is the number of cybersecurity awareness programs conducted and y is the total number of targeted cybersecurity awareness programs to be conducted	NA	NA	20	40	60	80	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

Level of cyber security awareness to Government employees This indicator intends to show the level of cyber security awareness among public institutions employees It will be calculated as (x/y)*100 where x is number of employees passed cyber security awareness test and y is total number of employees performed the cyber security awareness test	NA	NA	NA	NA	NA	NA	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA
Percentage of certified professional cyber security personnel in public institutions This indicator intends to show the trend of increase in certified cyber security professionals in public institutions It will be calculated as (x/y)*100 where x is the total number of certified cyber security professionals and y is the total number of targeted ICT Security Personnel conducted	NA	NA	20	40	60	80	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

OBJECTIVE: Management of Cyber Security Risks and Incidents Enhanced												
Percentage of public institutions with developed and operationalized Incident Response Management plans This indicator intends to show the trend of public institutions that developed and operationalized Incident Response Management plans This will be calculated by (X/Y) *100 where X= Number of public institutions that developed and operationalized Incident Response Management plans and Y = Total number of public institutions	NA	NA	NA	NA	20	60	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

Percentage of public institutions operationalizing ICT Risk Management Plan This indicator intends to show the trend of public institutions that operationalized The Government Risk Management Plan This will be calculated by (X/Y) *100 where X= Number of public institutions that operationalized the Government Risk Management Plan and Y = Total number of public institutions	NA	NA	NA	NA	20	60	100	e-GA	Interview, Key Informant	Annually	Government Cyber Security Strategy Implementation Report	Annually	PO-PSMGG/e-GA

Percentage of significant cyber security incidents responded by public institution based on their respective RTO and RPO This indicator intends to show the trend of Government systems that recover and get back to services quickly after ICT disasters. This will be calculated by (X/Y) *100 where X= Number of systems recovered to services based on their planed RTO and RPO and Y is total number of systems which encountered cyber security attacks.	NA	NA	100	100	100	100	100	Reports	Survey and Questionnaire	Semi-Annually	Reports	Annually	PO-PSMGG/e-GA

Percentage of critical systems monitored against cyber-attacks This indicator intends to measure the trend at which Government critical systems are monitored against cyber-attacks This will be calculated as: (X/Y)*100 where X = Number of monitored Government critical systems and Y = Total number of Government critical systems	NA	NA	100	100	100	100	100	Reports	Survey and Questionnaire	Semi-Annually	Reports	Annually	PO-PSMGG/e-GA
Percentage of identity theft / identy fraud redeced in the Government Transactions This indicator intends to measure the trend at which identity teft/identity fraud reduced in the Government transactional services This will be calculated as: (X/Y)*100 where X = Number of identity theft managed and Y = Total number of identity theft occurred	NA	NA	80	90	100	100	100	Reports	Survey and Questionnaire	Semi-Annually	Reports	Annually	PO-PSMGG/e-GA

1.2 Evaluation Plan

The Evaluation Plan consists of the evaluations to be conducted during the Strategy Cycle, description of each study, evaluation questions, the methodology, timeframe and the responsible person. The evaluations intend to obtain evidence as to whether the interventions and outputs achieved have led to the achievement of the outcomes as envisioned in the Strategy outputs. The Evaluation Plan matrix is detailed on Table 5 below:

Table 5: Evaluation Plan Matrix

No	Evaluation	Description	Evaluation Questions	Methodology	Timeframe	Responsible
1.	The Study on Protection of Government Systems, data and Infrastructure	This evaluation intends to examine extent of protection of Government Systems, data, Infrastructure, Systems and facilities	Are there operational standards and guidelines to protect Government information infrastructure and systems? Is there operational Government Public Key Infrastructure (PKI)? How much percentage of public institutions were connected Government Network (GovNet)? How much percent are critical Government systems exchange data through GovESB ? Are the security tools available? Are critical application systems and data hosted on approved hosting environment? What is the state or condition of e-Government Infrastructure security? Is there an adequate level of knowledge and awareness on protection of e-Government services? Is there sufficient collaboration and coordination of protection of Government ICT systems and infrastructure? Are there adequate Institutional cyber security controls deployed?	Surveys Questionnaires Interviews Focus group discussions Controlled studies Literature reviews	December, 2023	PO-PSMGG (DP)

2.	Building of Institutional Cyber-resilient	This evaluation aims at measuring the level of compliance in e-Government Cyber-security	Is there a guideline for Government electronic Data Management? Is there a guideline for Capability Maturity Framework for public institutions? Is there e-Government standards and guidelines to govern institutional cyber security resilience Are institutional Disaster Recovery Plans for Government's critical systems operationalized and periodically tested? How much Government critical systems were able to recover based on their RTO's and RPO's Is there an adequate level of monitoring of Government critical infrastructure against cyber-attacks? Is there operational Risk Management Framework by public institutions and how much is it implemented? Are there adequate tools to timely identify report and respond to cyber security incidents? Is there efficient and effective Cyber-security Team for e-Government in place? Are there competent cyber-security focal persons in the Public Institutions? What other interventions are needed to improve e-Government Cyber-security? How many Cyber-security incidents have occurred in the period of 2022/23 to 2026/27? Are there any Cyber-security initiatives that have been done from 2022/23 to 2026/27? What do you expect from the next Government Cyber-security strategy? Are there any legal issues that hinder Cyber-security initiatives implementations?	Surveys Questionnaires Interviews Focus group discussions Controlled studies Literature reviews	December, 2023	PO-PSMGG (DP)