September 2022

THE NATIONAL CYBERSECURITY POLICY OF THE GAMBIA 2022-2026

Revised Version

Contents

LIST OF ABBREVIATIONS

ICT	Information Communications Technology
ICI	Information Communications Infrastructure
NICI	National Information Communications Infrastructure
NCI	National Critical Infrastructure
ICT4D	Information Communications Technology for Development
NCII	National Critical Information Infrastructure
GICTA	Gambia Information Communications Technology Agency
GoTG	Government of The Gambia
KPI	Key performance Indicator
WARCIP	West African Regional Communications Infrastructure Program
GSC	Gambia Submarine Cable
ACE	Africa Coast to Europe Submarine Cable
GAMTEL	The Gambia Telecommunications Services Company
GM-CSIRT	The Gambia Computer Security Incident Response Team
CERT	Computer Emergency Response Team
SOC	Security Operation Center (constituent of GM-CSIRT)
NOC	Network Operation Center (sector network operation center)
NCSC	National Cybersecurity Commission
NCSA	National Cybersecurity Authority
NCSC	National Cybersecurity Committee
NCCD	National Cybersecurity Coordination Department
GNCSS	Gambia National Cybersecurity Strategy
NDP	National Development Plan
CMM	Cybersecurity Maturity Model
PURA	Public Utility and Regulatory Authority
MOCDE	Ministry of Communications and Digital Economy
GSC	Gambia Submarine Cable company
GPF	Gambia Police Force
MOJ	Ministry of Justice
ISP	Internet Service Provider
RNP	Regional Network Provider
MOD	Ministry of Defense
MOI	Ministry of the Interior
BCP	Business Continuity Plan PKI Public Key Infrastructure
NDP	National Development Plan

INTERNATIONAL COOPERATION

International Protocols

- Budapest Convention on Cybersecurity
- African Union convention on Cybersecurity and personal Data Protection (Malabo convention)
- ECOWAS Directive on fighting Cyber Crime within ECOWAS
- ECOWAS convention on mutual Assistance in Criminal Matters
- ECOWAS Convention on Extradition

EXECUTIVE SUMMARY

The use of ICTs and the Internet has become indispensable global tool for governments, businesses, civil society organizations and individuals. The Gambia as a country has one of the highest mobile phone concentrations in Africa with internet penetration rate estimated at 19.01 percent according to a study in 2016[1]. This rating indicates the country is witnessing rapid technology transformation. However, due to constant evolving technology and network environment, the demand on Internet broadband services and the increasing dependence on ICTs, creates condition for criminal misuse of the digital platforms against core security principles of Confidentiality, Integrity and Availability. It is a reality that cannot be ignored because of the dynamic nature and sophistication of attacks being perpetrated in cyberspace.

The actors are mainly attracted by political or financial motives, targeting and exploiting systems vulnerabilities. The consequences can be devastating on mission critical systems with potential to undermine ability of Government to function or perform essential services across multiple sectors. By extension, the scope of disruptions can go far beyond the ICT sector and the effects are usually loss of personal information, intellectual property, classified government information and reputational damage.

With our increasing dependence on technology and information infrastructures, the risk of exposure to cyber threats and potential attacks against critical information infrastructure and the impact on socio-economic wellbeing is a great source of concern.

[1] Cybercrime and Cybersecurity trends in Africa, Published November 2016

To mitigate this risk, The Gambia as a country needs a reliable governance structure, Cybersecurity cultured society and robust systems to support essential services in both public and private sectors of the economy.

Realizing the need to support cybersecurity initiatives, The government of The Gambia (GoTG) has committed itself to 'aggressively pursue a Cybersecurity prioritization strategy in its ICT4D Policy statements and objectives[2]. The move was intended to strengthen Gambia's Cybersecurity capacity, capabilities and enactment of appropriate legal framework. The policy objectives seek to generate and promote synergy for Cybersecurity governance, coordination, cooperation and collaboration between the public and private sectors, civil society and the citizenry. Therefore, having in place organized and coordinated response mechanisms will help reduce the risks of attacks on mission critical systems and provide safety and security in Cyberspace.

To achieve security assurance in this regard, requires a robust national capability at strategic, tactical and operational levels with **programs to Identify, Prevent, Protect, Detect, Respond and Manage Threats** to critical information infrastructures and services. The policy also envisions the harmonization of sectoral information security policies and programs including institutional foundations with a view to ensuring safety and security in ICT usage.

[2] The Gambia ICT for Development (ICT4D) or NICI- 2 Policy Statements, (2017-2026), WARCIP, December 2016

1. INTRODUCTION

The Government of The Gambia (GoTG) embarked on formulation of the county's Cybersecurity policy and strategies. This was in response to growing cyber threats and the need to strengthen protection for critical national infrastructure, services, individuals and businesses. The Gambia is witnessing transformation of digital platforms, ICT infrastructure development in public and private sectors of the economy. However, these technologies bring new types of threats ranging from information systems attacks, denial of service disruptions, and identity or information theft, Cyber Warfare among host of other crimes. These threats are increasing on a daily basis, with renewed sophistication.

Given the current level of investment in the ICTs and information systems in the country, it is imperative that information systems and critical infrastructure are secure and resilient against cyber-attacks. To be able to effectively mitigate the associated cyber risks, Government must put in place proactive measures in building robust systems to fight cybercrime.

It is in this context, the Gambia National Cybersecurity Policy shall establish an environment of trust and confidence in the use of Information Systems. The policy shall ensure Gambia is able to protect its interests in cyberspace to enhance national security. This will be achieved by providing assurance on confidentiality, integrity, availability of information assets and continuity of business operations.

The Ministry in charge of Cybersecurity (MOCDE) in collaboration with the relevant stakeholders took the lead in the formulation of The Gambia Cybersecurity Policy.

This policy shall be reviewed and implementation monitored and evaluated periodically to ensure both current and emerging threats are timely and appropriately tackled.

The document is organized as follows. Executive summary provides succinct conceptual framework, objectives and policy scope, followed by Introduction, policy context, Government initiatives, and current Cybersecurity status of The Gambia. The next Section explores the Policy, Vision and Mission, Guiding Principles, Strategic Objectives, Strategic goals, Policy Actions, Key Pillars, Institutional frameworks, financial and legal implications.

1.2. POLICY CONTEXT

Security of Gambia's cyberspace is an important pre-requisite for allowing the economy and social development of the people through harnessing of the fully benefits of digital transformation. In the last decade, Government of The Gambia (GoTG) has undertaken public policy initiatives intended to help transform the country into knowledge-based economy and ensuring national safety, security and prosperity in general. ICT and development are critical and important priority areas for the government especially in the realization of the long term vision to become a middle-income knowledge-based economy.

In the ICT4D (NICI_2) policy, Cybersecurity is a key priority for ensuring secure management of all deployed ICTs in particular Critical National Infrastructure assets supporting Gambia's ICT goals.

In 2012, GoTG commissioned its first submarine cable (GSC) through West African Regional Communication Infrastructure Programme (WARCIP). The objective was to increase the capacity of broadband networks through global network of broadband Fibre optics infrastructure at more than 100GB; improve internet connectivity and to reduce costs of communications services in The Gambia.

To further compliment the breakthrough and to ensure reliable internet penetration throughout the country, GoTG embarked on the implementation of the ECOWAN Project. This was a national Fibre optic backbone of about 947km that lay on both sides of the River Gambia.

The Gambia Telecommunications Services Company (GAMTEL) a national telecommunications Company and the Gambia Submarine Cable Company (GSC) are all major stakeholders in the national Cybersecurity efforts. These initiatives brought unprecedented transformation to the country's broad-band network expected to provide high speed access to services in the interior of the country.

In 2017, Gambia ICT for development (ICT4D) policy was formulated as succeeding policy to (NICI-1)[3]. It was developed, validated and adopted by cabinet in 2018. The review of (NICI-1) policy was commissioned in 2016, and resulted to remarkable improvement of ICT infrastructural deployment across the country. However, this achievement did not impact much in the public and private service delivery in terms of efficiency and speed and in particular online content and application deployment to further provide the needed e-government and e-commerce services to the population.

Next, the Gambia Government adopted The Gambia ICT for Development Policy 2018-2028 focusing on eight priority areas; capacity building, private sector development, gender equality and youth empowerment, agricultural development and climate change including broadband and cybersecurity.

[3] National Information Communication Infrastructure (NICI 1-2), MOCDE, 2017

Broadband and Cybersecurity components have been included in the last pillar of the ICT4D policy statements as a new emerging thematic area. Given their importance, a separate treatment is accorded to each area and every pillar requires a 5-year strategic plan to guide successful implementation.

In order to facilitate the operationalization of ICT4D Policy, GoTG envision the formulation of the ICT for Development Master Plan. The plan shall incorporate both remedial and proactive measures necessary to create opportunities for Gambians to create wealth and enhance the quality of living of the citizenry.

The Cybersecurity policy creates a framework for defining and guiding the actions related to the security of the Cyberspace. The policy framework shall provide the foundation required to ensure that public and private sector initiatives continue to receive support throughout the implementation of the vision set in the strategic document.

During the policy formulation best practices have been adopted from national, regional and International conventions and protocols on Cybersecurity. These include review of existing national policies, International Telecommunications Union (ITU) cybersecurity documents, Africa Union (AU) “Malabo Convention ” and Economic Community of West African States (ECOWAS) cybersecurity directives and in addition, the recommendations advanced by Cybersecurity Capacity Review The Gambia Maturity Model (CMM) framework.

1.3. GOVERNMENT INITIATIVES

The Government of The Gambia (GoTG) recognizes the positive role of ICT as a crosscutting enabler for all development sectors of the economy, and thus holds the view that opportunities in ICT has potential to improve standards of living of Gambian citizenry. To this end, several initiatives on policies, strategies and action plans were embarked upon at both sector and national levels.

In addition, it has also put in place strong public policy agendas towards the socio-economic development of the country leveraging ICTs as key crosscutting enablers:

1.3.1 The National Development Plan (NDP) and Gambia Vision 2020

The National Development Plan NDP 2018-2022 states "Government will strive to build local capacity including Cyber Defense Systems and personnel to protect national security. Vision 2020 blueprint further establishes a goal to raise the standard of living of Gambians by transforming the country's economy into an information-rich, service-oriented, knowledge-based middle income country.

1.3.2 Poverty Reduction Strategies - (SPA I and SPA II)

These are socio-economic development strategies focusing on poverty reduction to drive Gambia's social and economic development to achieve national economic objectives.

1.3.3 Programme for Accelerated Growth and Employment (PAGE) or (PRSP III)

The overall objective of this initiative is to accelerate growth and employment based on the following five pillars:

- Accelerating and sustaining economic growth;
- Improving and modernizing infrastructure;
- Strengthening human capital and enhancing access to social services;
- Improving governance and increasing economic competitiveness; an
- Reinforcing social cohesion and mainstreaming cross-cutting issues.

1.3.4 The National Information and Communication Infrastructure (NICI 1-2) Policy

NICI-1 Policy statements and subsequent action plans (The ICT4D-2013) seeks to drive the nation's ICT for Development (ICT4D) agenda towards information and knowledge-based economy and society.

NICI 2: The National ICT for Development (ICT4D- NICI 2) focuses on leveraging the existing infrastructure and environment to improve service delivery as well as enhance Cybersecurity for The Gambia

Based on the afore-mentioned, there is indication of growing transformation and investment in ICT infrastructure and applications to consider as critical information assets for The Gambia. As a result, there is increasing dependency on the proper functioning and operation of ICT infrastructure in all sectors. This includes, but not limited to reliance on the Internet for e-Government services, e-Commerce, e-Banking and other ICT-based services. In addition, the Gambian society is slowly becoming dependent on ICT for business, health, education, agriculture, and other sectors. The protection and availability of these critical assets are paramount. Cybersecurity has thus become a strategic national priority affecting all levels of society.

In this context, enhancing cybersecurity to protect critical information infrastructures is essential to national security and economic wellbeing. Securing The Gambia's cyberspace thus requires comprehensive, collaborative efforts to deal with Cybersecurity at all levels. This calls for an appropriate and comprehensive Cybersecurity policy framework and strategies to ensure security and resilience of national information systems and services.

1.4. STATUS OF GAMBIA'S CYBERSECURITY

The Gambia Government recognizes the importance and danger posed by cyber criminals. In order to ensure safety and protection of citizens from cyber threats, it becomes a collective responsibility of all stakeholders to protect Gambia's cyber-space. In order to achieve strategic objectives, there is need for a strong institutional framework to harmonize and coordinate initiatives with an integrated approach.

The absence of strong institutional framework has often led to inconsistency and duplication of efforts among stakeholders. In terms of Policy, Legal, and Regulatory Framework and Standards governing ICT, issues related to ICT Services and Security of critical infrastructure and systems must be address.

The Government of The Gambia has undertaken important steps in this direction. For example, steps to enhance cybersecurity capabilities and incorporated cybersecurity in the national agenda. The measures taken by The Gambia indicate work in progress. The measures include the formulation of Cybersecurity policy & strategies and Action plans, Institutional Governance framework, Cybercrime Bill 2019 among others.

The Gambia Information and Communication Act 2009 is general in scope, comprehensive; but lack substantive and procedural laws on cybercrime. This gap has been captured in the new cybercrime bill 2019. The adoption of national cybersecurity standards is another issue to be addressed. The use of standards as a measure of best practice is non-existent in some sectors of government. This has resulted to inconsistencies in information security assurance practices in both public and private sectors.

The draft National cybersecurity strategy provides for establishment of institutional framework. These include The Gambia Information Communication Technology Agency (GICTA), National Cybersecurity Coordination Directorate (NCCD), Gambia Computer Security Incident Response Team (GM-CSIRT) and National Cybersecurity Committee (NCSC). All these institutions shall help enhance and protect critical infrastructure including the National Fibre Backbone, Data Center NDC/Serekunda Exchange, SIXP (ISPs last mile networks), e-Government Systems, Energy Infrastructure, Banking and Financial systems etc.

In addition, Government shall promote initiative to build Cybersecurity Capacity, as well as to improve its capability. This also requires development and implementation of education and training programs, cybersecurity policy and strategy including cooperation, and collaboration with international partners to ensure knowledge and skills transfer. Although, these initiatives sounds remarkable; there are areas that require improvement such as skills. It is also important to establish a Cybersecurity culture and awareness among citizens as majority of public sector employees have low level of cybersecurity awareness. Although, the private sector operators and financial institutions have taken initiatives to address cyber threats. Generally, low-level awareness of cyber risks and threats is apparent in public, private, civil society and academia.

2. NATIONAL CYBERSECURITY POLICY

The Gambia National Cybersecurity Policy shall establish a conducive environment that provides trust and confidence in the use of ICT facilities as well as ensure Gambia is able to protect its national security in cyberspace.

2.1 VISION

A Gambia with a secure, resilient, and trusted cyberspace for enhanced inclusive socio-economic development.

2.2 MISSION

To create an enabling environment that ensures the protection of Critical National Infrastructure, Information Systems and Users with effective capabilities for accelerated responses to cyber risks and threats.

2.3 GUIDING PRINCIPLES

For the mission to succeed, it must be supported by the following guiding principles:

- **National Leadership** – The scale and complexity of Cybersecurity requires strong national leadership and support;
- **Roles & Responsibilities** – All ICT users including government, businesses and citizenry should take due diligence measures to secure their own information and information systems, and have an obligation to respect the information systems of other users;
- **Public-Private Collaboration** – A collaborative approach to Cybersecurity across government and the private sector is essential and crucial for ensuring national coordinated response;
- **Risk-Based Management** – There is no such thing as absolute Cybersecurity as security is a process in its own right. The Gambia must therefore apply a risk-based approach to assess, prioritize and provide resources for Cybersecurity activities.
- **Gambian Values** – The Gambia government must pursue and implement Cybersecurity policies and strategies that protect the Gambian cyberspace, citizenry, economy and the overall policy vision.
- **International Cooperation** – The trans-national nature of cyber threats makes it essential to promote international cooperation and collaboration in the fight against cybercrime. The Gambia supports and will actively contribute to international Cybersecurity initiatives.

2.4 Strategic Objectives

For the goals set in the policy to be realized, the following five (5) strategic policy objectives must be addressed.

Strategic Objective 1: Cybersecurity Policy and Strategy

To enable and facilitate the formulation and Implementation of appropriate policies, strategies and programs for a secure, resilient and development oriented digital ecosystem within a period of two years.

Strategic Objective 2: Cybersecurity Culture and Society

Establishing cyber-hygiene best and cybersecurity culture for ensuring safety and confidence in the Cyberspace

Strategic Objective 3: Cybersecurity Education, Training and Skills

To develop cybersecurity capacity building programmes for ensuring, the availability, quality, uptake of educational and trainings for stakeholders by 2023

Strategic Objective 4: Legal and Regulatory Framework

To formulate and strengthen cybersecurity, Legal and regulatory frameworks with enforcement mechanisms for enhanced resilience in the cyberspace

Strategic Objective 5: Standards, Organization and Technologies

To develop and adopt cybersecurity standards for best practices in mitigation of Cybersecurity risks

2.5. Strategic Goals

- Strengthened Legal and Regulatory Frameworks that promotes compliance with appropriate technical and security standards.
- A trained, educated, aware and informed Cybersecurity cultured society at all sectors and levels within the country, that promotes information sharing and collaboration on cyber security.
- Established Institutional Framework that fosters cyber-security coordination and enhances the fight against all forms of Cybercrime.
- Existence of strong Cybersecurity capabilities, capacities and infrastructure for prevention, protection, detection, and response to cyber**s**ecurity incidents and threats.

- Continued protection of Information Systems in particular critical information infrastructure and services that ensures the safety of vulnerable groups in cyberspace, especially those of children.
- Foster National and International Cooperation in the field of Cyber security.

2.5 POLICY SCOPE

This Policy covers cybersecurity governance, legal measures, law enforcement, national security and critical national infrastructure protection, awareness raising, education and training and standardization.

2.5.1 Gambia's National Critical Infrastructure (GNCI)

The National infrastructure is a critical business driver to any nation's economic survival. To ensure protection and resilience of NCIs, development of national cybersecurity strategy and programs is fundamental. The Gambia National Critical Information Infrastructures are located in the following key sectors:

Gambia's National Critical Information Infrastructure (NCII) Sectors	
• Banking and Finance • Information and Communications • Power and Energy • Health Services • Water and Food services	• National Defense and Security • Transport • Government Agencies • Emergency services

2.5.2 Components of Gambia's Cyberspace:

The country's cyberspace are those digital infrastructures that interconnect national, regional and global information and communications networks. These components are identified as follows:

Components of Gambia's Cyberspace	
• Enterprise Networks/ Intranets, Services, • Local Internet Service Provider (ISP), SIXP • Regional Network Providers (RNP), • Internet Backbone, • National Data Centre (IFMIS)	• Gambia sub-marine cable and NBN Data Centre • Online Content • Sources of Online Content • End-Users • Telecommunication Services

3.0 POLICY STATEMENTS

3.1 Effective Governance

Government of The Gambia (GoTG) will centralize coordination of national Cybersecurity initiatives and promote effective cooperation between public and private sectors. In order to sustain the gains from these initiatives, a National Cybersecurity Coordination Directorate (NCCD) shall be established under GICTA for formal coordination and information sharing.

3.2 Legislative and Regulatory Frameworks

The Ministry of Communications and Digital Economy (MOCDE) and relevant stakeholders shall collaborate with the Ministry of Justice to ensure regular review and enhancement of Gambia's Cyberspace legislation for purposes of preventing or reducing potential threats to Cyberspace.

In order to empower national law enforcement agencies to effectively prosecute cybercrimes, GoTG shall establish a sustainable capacity building programs to

acquire new skills and effective ways of enforcing cyber laws. The Government shall further ensure that all applicable national legislation is complementary and in compliance with regional, international treaties, protocols or conventions.

3.3 Cybersecurity Technology Frameworks

GoTG shall put in place uniform policy measures to develop a national Cybersecurity technology framework that specifies Cybersecurity requirement, controls and baselines for Critical national Information Infrastructure (CNII) elements. This will be followed by protective mechanisms to implement and evaluate Certification programs for Cybersecurity products and systems.

3.4 Security Culture and Capacity Building

GoTG shall invest resources needed to develop, foster and maintain a national culture of Cybersecurity. As part of the process of development of culture on Cybersecurity, GoTG will support the standardization and coordination of Cybersecurity awareness and education programmes across all elements of the Cyberspace.

The national awareness shall include civil society and national coordinating agencies. Government shall also establish an effective mechanism for Cybersecurity knowledge (Intelligence) dissemination at the national level and identify minimum requirements and qualifications for information security professionals.

3.5 Research and Development

To become self-reliant in protecting the Cyberspace to a level commensurate with the risk, government shall formalize the coordination and prioritization of Cybersecurity research and development initiatives. It will further enlarge and strengthen the Cybersecurity research community. Strategic research and development shall be encouraged by promoting the development and commercialization of intellectual properties, technologies and innovations

through focused research and development. Government shall also put in place programmes to promote the growth of Cybersecurity industry in the country.

3.6 Compliance and Enforcement

In order to ensure compliance and enforcement, unified policy measures and mechanism shall be put in place to standardize Cybersecurity systems across all elements of Gambia's Cyberspace. Government will also strengthen the monitoring and enforcement of standards as well as develop a standard Cybersecurity Risk Assessment Framework.

3.7 Cybersecurity Emergency Readiness

To ensure Cybersecurity emergency readiness, GoTG including all stakeholders shall develop effective Cybersecurity incident reporting and Crisis management mechanism. This shall include among others the development and strengthening of the Gambia Computer Incidence Response Team (GM-CSIRT) and sectoral Computer Incidence Response Team (CSIRT) in the dissemination of vulnerability notices and threat warnings in a timely manner. Government shall also ensure development of a standard business continuity and recovery management framework (BCP). GoTG shall further encourage monitoring of all elements of the Cyberspace.

3.8 International Cooperation

GoTG shall promote active participation in all relevant international Cybersecurity forums and multi-national agencies initiatives. GoTG shall make every effort to promote active participation in all relevant international Cybersecurity activities by hosting International Cybersecurity Conferences and conducting periodic cybersecurity workshops and seminars.

4.0 KEY POLICY PILLARS

4.1 PILLAR 1 – BUILDING CYBER SECURITY CAPABILITIES

Objective: Build cybersecurity capabilities to manage Cyber-incidents and respond promptly to cyber threats.

4.1.1 Measures

I) Establishing Gambia Computer Security and Incident Response Team;

The Gambia Computer Security and Response Command Center shall be designated to Gambia Computer Security and Incident Response Team referred as "GM-CSIRT". The GM-CSIRT will be strengthened to prevent, protect, detect and respond to Cybersecurity threats and will play a leading role in managing incident response or crisis situation. GM- CSIRT operational capabilities in terms of capacity building, and other vital technology resource shall be strengthened.

II) Develop National Cyber Contingency Plan:

A National Cybersecurity Contingency Plan (NCCP) shall be put in place to provide measures for responding to and recovering after major incidents that involve Critical Information Infrastructure (CII) or information systems. NCCP shall outline the criteria to be used to identify a crisis, define key processes and actions for handling the crisis, and clearly define the roles and responsibilities of different stakeholders during a Cybersecurity crisis.

III) Establish Cybersecurity Capabilities within Institutions:

Depending on the size and complexity of information technology infrastructure and systems, public and private organizations shall establish a Cybersecurity function within the IT units, responsible for planning and implementing Cybersecurity programs.

4.2 PILLAR 2 – INSTITUTIONAL FRAMEWORK FOR CYBERSECURITY GOVERNANCE AND ENHANCEMENT

Objective: To build Cybersecurity capabilities and secure national information assets requires a sound governance structure for effective coordination of national Cybersecurity initiatives in order to safeguard Government information systems and services against cyber-attacks.

4.2.1 Measures

I) The complexity of Cybersecurity threats is such that the need for strong institutional framework to coordinate Cybersecurity initiatives with an integrated approach is crucial. The absence of such framework has often led to inconsistency and duplication of efforts among stakeholders. Therefore, GoTG shall, as a temporal measure establish a centralize Cybersecurity Coordination Directorate within GICTA to be responsible for the development, implementation and coordination of the national Cybersecurity initiatives. However in the interest of international good practice and depending on level of national cyber threat profile in scope and sophistication, a national Cybersecurity Agency or Authority shall be establish to effectively tackle the growing Cybersecurity demands of the country.

II) Establish a National Cybersecurity Advisory Board;

In order to establish strong Cybersecurity governance framework, the GoTG shall put in place a National Cybersecurity Commission/Committee (NCSC). This commission/committee shall provide coordination and strategic guidance on matters related to National Cybersecurity. The composition of the Commission shall be multi-sectoral; involving public, private and civil society stakeholders relevant to Cybersecurity.

III) Information Security Assurance or Compliance

The NCCD and GM-CSIRT in charge of Cybersecurity coordination and response shall establish the Government Information Security Certification (GISC) program based on Government Security Architecture (GSA) to enhance Information Security Management System in public institutions.

GM-CSIRT shall conduct periodic Information Security Audit in consultation with the National Audit Office. Private institutions will be subject to a mandatory information security audit at least once a year in accordance with ISO 27001/27002 implementation or other open standards (ITIL, CoBIT frameworks, etc.). They shall equally seek support from the NCCD - GM-CSIRT in charge of cybersecurity.

IV) Establish security classification for systems, applications and services

The NCCD- GM-CSIRT shall define security classification levels of systems, applications and services for GoTG. More especially, e-Government services must adopt appropriate cybersecurity technology and improve their overall security capability. The security level of e-Government services shall be based on the risk-based assessment.

V) Establish secure and reliable environment for e-Government and e-commerce with National Public Key Infrastructure;

The GoTG shall promote the use of national Public Key Infrastructure (PKI) in order to establish a secure and reliable environment for e-Government and e- Commerce through PKI technology based security services such as authentication, data integrity, confidentiality, and non-repudiation.

In collaboration with other stakeholders, GICTA shall put in place laws, regulations, policies and standards that promote use of national PKI.

The Gambia ICT Agency (GICTA) shall manage the Root Certification Authority (Root CA) and licensing of PKI services and shall define the requirements for Accredited Certification Authority (ACA) and usage of digital certificates.

The GM-CSIRT shall be accredited as the GoTG certification authority. In collaboration with other certification Authorities, it shall promote the usage of digital certificates in critical e-Government services, e-Commerce, e-Banking, e-Healthcare systems as well as other Sectors.

4.3 PILLAR 3 – CYBERSECURITY LEGAL AND REGULATORY FRAMEWORK

Objective: To strengthen existing legal and regulatory framework to adequately address cyber-crime and facilitate the criminalization of acts related to cyber-crime that are not addressed by existing law, yet pose a potent threat to national security.

4.3.1 Measures

I) Strengthen legal and regulatory framework;

There is a need to enhance the current legal and regulatory framework to facilitate the enforcement of Cybersecurity laws, investigation and prosecution of cyber-crime related activities.

To this end, the GoTG shall review the existing legal and regulatory framework to ensure that all applicable national legislations incorporate Cybersecurity provisions that grant reasonable capacity to national law enforcement agencies, which are complementary to, and in harmony with, international laws, regional treaties and conventions. The GoTG will also strengthen the legal and regulatory framework to prevent Cybersecurity threats arising from harmful online content dissemination in the national cyberspace.

II) Standards and Guidelines: To ensure information security good practices in public and private institutions, the GM-CSIRT shall develop and adopt standards and guidelines in collaboration with Gambia Standards Bureau and benchmarked with international standards such as (ISO/IEC 27001/002 (Information Security Management Systems Requirement), ISO/IEC9000 (Quality Assurance), ISO14000 (Environment), ISO/IEC27037 (Cybersecurity)) or UK-ACPO (Association of Chief Police Officers – Forensics Investigations)) Best Practice Guidelines for digital Forensics Investigation among host of other open standards. The public and private sector stakeholders shall adopt unified and consistent Cybersecurity standards.

4.4 PILLAR 4 – CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Objective: To protect National Critical Information Infrastructure against cyber-attacks and related cybercrimes to ensure Confidentiality, Integrity and Availability of essential services.

4.4.1 Measures

I) Protect National Critical Information Infrastructure;

The disruption of Critical Information Infrastructures (CIIs) has direct impact on businesses and society. Therefore, GICTA shall put in place a mechanism to ensure that National Critical Information Infrastructure (CII) is defined and secured against various cyber threats.

MOCDE in collaboration with the Gambia ICT Agency (GICTA), NCCD, MOJ, PURA, including other relevant Sector to Cybersecurity shall develop the CII Information Protection law, CII regulations, compliance, and protection plan, among others. CII regulation shall address, but not limited to CII procedures manuals, access control, business continuity and contingency plan, physical and logical protection mechanisms.

II) Establish Public-Private Sector Collaboration Framework

Given the role private sector plays in the development and management of ICT infrastructure and services, collaboration with the private sector is central in addressing issues of Cybersecurity and resilience. The GICTA - NCCD shall put in place a framework that defines the roles and responsibilities of organizations managing critical Information Infrastructure. The GoTG and private sector will meet regularly to discuss and review the security status of CIIs and share knowledge on Cybersecurity related issues.

4.6 PILLAR 5 – CYBERSECURITY CAPACITY BUILDING AND AWARENESS

Objectives:

- Build Cybersecurity prevention and response capabilities;
- Create Cybersecurity awareness for Gambian citizens.

4.6.1 Measures

I) Cybersecurity Capacity Development

Cybersecurity threats are dynamic and complex to mitigate and require a comprehensive program of continuous development of human capacity and retention policy. To ensure a sufficient level of expertise in the field of Cybersecurity across the public and private sectors, the GM-CSIRT shall develop and implement a cybersecurity capacity-building program. In this program a workforce of professionals skilled in Cybersecurity will be created through capacity building, skills development and continuous professional training and development.

II) Develop a National Cybersecurity Awareness Program

It is important that Gambian citizens using or operating information assets understand the threats and risks in cyberspace. GM-CSIRT shall develop a Cybersecurity awareness program for institutions and individuals as well as encourage ownership. GM-CSIRT will coordinate and collaborate with The

Gambia Cybersecurity Alliance (GCSA) and other civil society organizations for the advocacy campaign.

4.7 PILLAR 6 – BUILDING A CYBERSECURITY INDUSTRY

Objective: Develop a stronger Cybersecurity industry to ensure a resilient Gambian cyberspace.

4.7.1 Measures

I) Foster Innovation through Research and Development

In collaboration with the University and the industry, a Cybersecurity Research and Development (R&D) program shall be developed. The Research and Development program shall focus on the development of intelligent intrusion prevention and detection systems, Digital Forensics, Cryptography, Encryption technologies and wireless security.

In a bid to nurture the growth of Cybersecurity industry, the products and services resulting from Cybersecurity innovations shall be commercialized within and outside The Gambia.

The R&D programs shall also address aspects related to development of trustworthy technology security systems and solutions, security evaluation of emerging technologies and devices, and research on emerging cyber threats. GICTA working with the Gambia Standards Bureau shall develop a standard quality assurance benchmark for all ICT products or appliance in The Gambia

II) Promote and strengthen the private sector participation in Gambia's Cybersecurity industry development.

To develop a stronger Cybersecurity sector or industry, a public private partnership shall be established to develop Cybersecurity services, skills and expertise that respond to Cybersecurity objectives. This will enhance Gambia's

capacity to provide services and skills inside and outside of the country in the Cybersecurity field.

4.8 PILLAR 7 – INTERNATIONAL COOPERATION

Objective: To establish a Regional and International Cooperation Framework to protect national Cyberspace.

4.8.1 Measures

I) Promote and Strengthen National and International Collaboration;

International investigations depend on reliable means of cooperation and effective harmonization of laws. National Cybersecurity Coordination Directorate through MOCDE shall continually enhance international cooperation in Cyber law and in response to cyber threats. NCCD and GM-CSIRT will support and participate in international research projects and the exchange of experts in Cybersecurity to enhance capabilities.

5. INSTITUTIONAL FRAMEWORK FOR IMPLEMENTATION

Securing Gambia's national information assets requires an adequate and comprehensive governance structure for focus and coordination of national Cybersecurity initiatives. It is therefore necessary to establish an efficient coordination mechanism for effective Cybersecurity.

The Cybersecurity implementation framework is composed of the Gambia ICT Agency (GICTA), National Cybersecurity Coordination Directorate (NCCD), Gambia Computer Security Incident Response Team (GM-CSIRT), National Cybersecurity Commission/Committee (NCSC) supported by ICT units within public and private sector institutions.

5.2. INSTITUTIONAL ROLES

This section describes the roles and responsibilities of stakeholders involved in the implementation of this Policy.

5.2.1 MINISTRY OF COMMUNICATIONS AND DIGITAL ECONOMY

This Ministry is the overall national authority responsible of Cybersecurity for The Gambia

5.2.2 GAMBIA INFORMATION COMMUNICATION TECHNOLOGY AGENCY (GICTA)

This Agency shall be responsible for the implementation of all national ICT matters including Cybersecurity Regulations through NCCD and GM-CSIRT.

5.2.3 NATIONAL CYBERSECURITY COORDINATION DIRECTORATE (NCCD)

This Directorate shall be established under GICTA to organize governance and implementation of the Cybersecurity strategy. The NCCD shall advise the permanent secretary MOCDE as well as proposes within the limits set by government, the appropriate rules, regulations, measures or standards to be implemented to protect critical infrastructures and to ensure security of networks and information systems. NCCD shall have authority over the GM-CSIRT but directly answerable to GICTA. NCCD will also collaborate with national Cybersecurity Commission/Committee to jointly coordinate the implementation of the Strategy.

5.2.4 THE NATIONAL CYBERSECURITY COMMSSION/COMMITTEE (NCSC)

The National Cybersecurity Commission shall be establish to provide leadership, oversight and guidance on implementation and development of national Cybersecurity strategy and reports to MOCDE. It is critically important that NCSC is inclusive of major stakeholders. Composition of the NCSC shall be reviewed to ensure members of the commission/committee are the most relevant and active stakeholders on Cybersecurity.

5.2.5 THE GAMBIA COMPUTER SECURITY AND INCIDENT RESPONSE TEAM (GM-CSIRT)

The GM-CSIRT shall be responsible for regulation of the Cybersecurity sector. It shall ensure institutional conformance to information security standards, guidelines and best practices necessary to secure Gambia's Cyberspace. It shall

act as the governmental and national operational Cybersecurity Command Centre. GM-CSIRT shall report to PURA-MOCDE and NCCD. It shall also conduct Cybersecurity audits, assessments and readiness exercises/drills for government institutions and develop security standards and best practices in collaboration with the Gambia Standards Bureau.

GM-CSIRT shall further conduct research on technical issues, support awareness campaigns and provide Cybersecurity training programs. GM-CSIRT shall operate and maintains national Cybersecurity infrastructure and systems and provides technical support to institutional Cybersecurity units or sector CSIRT. By extension, GM-CSIRT shall represent Gambia on international Cybersecurity fora. It shall also coordinate and support Government Ministries, Agencies and private sector institutions develop and enhance their Cybersecurity capabilities as well as implementation of this Policy.

6.0 FINANCIAL AND LEGAL IMPLICATIONS

6.1. FINANCIAL IMPLICATIONS

The National Cybersecurity Policy outlines different initiatives that will demand financial resources for implementation. The Government of the Gambia shall allocate a reasonable budget to ensure the effective implementation and review of the strategic objectives and action plan of the final NCSS. The NCCD shall spearhead the implementation of this Policy answerable to GICTA. The NCCD shall have the responsibility to define the short and long-term Strategic Plan and budget allocations.

6.2. LEGAL IMPLICATIONS

The approval of this Policy shall require an endorsement or approval of Cabinet. Furthermore establishing legislation and regulatory frameworks would require both enactment by parliament and approval of MOCDE, respectively. This will be preceded by review of existing legal framework to ensure that all applicable

national legislations incorporate Cybersecurity provisions, to follow the normal law reform process and procedure as well as consultations.