GAMBIA
NATIONAL CYBER SECURITY POLICY
2020 - 2024

Commissioned by
The Ministry of Information and Communication Infrastructure

SUBMITTED BY:

LASTING SOLUTIO
Providing business solutions that

JUNE 2020

infor@lastingsolutions.gm

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 Cyber Security Commission
NCSA	National Cybersecurity Authority
NCSC	National Cybersecurity Committee
NCCD	National Cybersecurity Coordination Directorate
GNCSS	Gambia National Cybersecurity Strategy
NDP	National Development Plan
CMM	Cybersecurity Maturity Model
PURA	Public Utility and Regulatory Authority
MOICI	Ministry of Information Communications infrastructure
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 broadband has become indispensable tools for government, businesses, civil society organizations and individuals. The widespread deployment and usage of Information and Communications Infrastructures (ICI) as a necessary precondition for rapid and sustainable socio-economic development is affirmed in the Gambia National ICT for Development (ICT4D) Policy and Strategy 2016.

The Gambia has one of the highest mobile phone concentrations in Africa with internet penetration rate of 19.01 percent according to a study in 2016[1]. This rating indicates the country is witnessing rapid technology transformation. However, with the growth of the Internet and multi-media services, new opportunities for perpetrating cybercrime are globally on the increase. This phenomenon involves exploitation of systems vulnerabilities in a constantly evolving technology environment. These vulnerabilities leads to further exposure to attacks and criminal access to personal information, intellectual property, and classified government-held information for financial gain or other forms of malicious intent.

As our level of dependence on technology and information infrastructures increases, continuous exposure to cyber threats against critical information infrastructure, socio-economic wellbeing, stability and national security is a great concern. By extension, the impact of a significant disruption to Critical Information Infrastructure (CII) could extend far beyond the ICT sector. It can affect the ability of Government to perform essential services and or missions in multiple sectors. Ultimately, the effect can be devastating on the national economy, public safety, social and national security in general.

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

Therefore, with our society becoming more interconnected and dependent on Internet services and ICTs, potential misuse of these technologies against core security principles of Confidentiality, Integrity and Availability is a reality that cannot be ignored given the sophistication of cyber threats and cyber-attacks against safety and security. To mitigate this challenge, The Gambia as a country would need reliable and robust systems to jointly support essential services in critical public and private sectors of the economy.

To support these efforts, GoTG has expressed commitment to 'aggressively pursue a Cyber security prioritization strategy in its ICT4D Policy statements and objectives[2]. This is intended to strengthen both the Gambia's cyber security capacity and capabilities targeted at promoting the development and enactment of appropriate legal framework. The policy objective seeks to generate and promote synergy for coordination, cooperation and collaboration between the public, private sectors, civil society and the citizenry in ensuring protection of critical national information infrastructures.

The motivation is to build 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. The policy also envisions the harmonization of national cyber security policies and programs including institutional foundations for cyber infrastructure protection across all sectors**.**

[2] The Gambia ICT for Development (ICT4D) Policy Statement 2018-2028

1. INTRODUCTION

The government of The Gambia (GoTG) embarked on development of Gambia's cyber security policy and strategy in response to growing cyber threats and the need to improve cybersecurity protection for individuals, businesses, government and critical national infrastructure. The Government recognized ICT as a key enabler for economic growth and social mobility. This is expected to improve standard of living of the Gambian citizenry and the national economy as a whole.

Currently, the Gambia is witnessing gradual transformation in ICT development in both public and private sectors. However, these technologies also come with new types of threats ranging from information systems or infrastructure attacks, denial or service disruptions, identity or information theft, Cyber Warfare among host of others. These threats are increasing on a daily basis, sophisticated and difficult to mitigate.

In this context, threats of cyber-crime against critical infrastructure and national Security in general demands for proactive measures by Government in preventing, protecting and responding to evolving cyber threats. In addition, given the current level of investment in the ICTs and information systems in the country, it is imperative that information systems and critical infrastructures are secure and resilient against cyber related threats.

The Gambia National Cyber Security Policy will establish an environment of trust and confidence in the use of ICT facilities as well as ensure that Gambia is able to independently protect its interests and enforce national security. This policy will guarantee confidentiality, integrity and availability of information assets and continuity of business operations. By extension, protect classified Government information, businesses and individuals and civil society organizations.

The Ministry in charge of national cyber security (MOICI) in collaboration with the relevant stakeholders took the lead in the development of The Gambia Cyber Security Policy. The policy will periodically be reviewed and implementation progress monitored to ensure that current and emerging threats are timely and appropriately addressed. This Policy document is organized as follows. The Executive summary provides succinct conceptual framework, objectives and policy scope. This is followed by an Introduction, policy context, Government initiatives, Current Cyber security status of The Gambia and guiding principles upon which the strategy is built on. The next Section explores The Gambia Cyber Security Policy, Vision and Mission, Strategic Objectives, Policy Statements and Key Policy Dimensions. The Final part explores Institutional framework, 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 to fully benefit from digital transformation. In the last decade, Government of The Gambia (GoTG) has undertaken public policy initiatives geared towards transforming the country into knowledge-based economy and ensuring safety, security and prosperity in general. Cyber security has since been an important priority for the Gambia government especially in the realization of the long term vision of The Gambia to become a middle-income knowledge-based economy. In the ICT4D (NICI_2) policy, Cyber Security is identified as a key priority to ensuring secure management of all deployed ICT including Critical National Infrastructure assets that support Gambia's ICT goals.

In 2012, the GoTG commissioned its first submarine cable (GSC) through the West African Regional Project (WARCIP). The objective was mainly 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 Gambia Submarine Cable (GSC) breakthrough and to ensure a reliable internet penetration throughout the country, GoTG embarked upon implementation of the ECOWAN Project. This is 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 cyber security efforts. These initiatives brought unprecedented transformation to the country's broad-band and 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). It was developed, revised and adopted by cabinet in 2018. The decision to review (NICI-1) policy was commissioned in 2016, and resulted in the 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.

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

Broadband and Cybersecurity 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 should incorporate both remedial and proactive measures necessary to create opportunities for Gambians to create wealth and enhance the quality of living of the citizens.

The cyber security policy for The Gambia will create a framework for defining and guiding the actions related to the security of cyber space. The policy framework will provide the foundation required to ensure that initiatives by public and private sectors continue to enjoy consistent support throughout the implementation of the vision set in the strategic document.

This cyber security policy is developed based on national, regional and International best practices from International Telecommunications Union (ITU), Africa Union (AU) and Economic Community of West African States (ECOWAS) directives and in particular 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, and thus holds the view that opportunities in ICT has potential to improve standards of living of Gambian citizenry. To this end, GoTG embarked on several initiatives for the development of policies, strategies and plans at sector and national level. By extension, it has strong public policy agendas towards the socio-economic development of the country, utilizing ICT as key crosscutting enablers: These public policies include:

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

The National Development Plan NDP 2018-2021 states that “Government will strive to build local capacity including Cyber Defence 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 cyber security for The Gambia

In view of the afore-mentioned, there is growing transformation and investment in ICT infrastructure and applications considered 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 is 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 and as such, cyber security has become a strategic national priority affecting all levels of our society. In this context, enhancing cyber security to protect critical information infrastructures is essential to national security and economic wellbeing.

Securing The Gambia's cyberspace requires comprehensive, collaborative and collective efforts to deal with cyber security at all levels. This calls for an appropriate and comprehensive cyber-security policy framework and strategies to ensure security and resilience of national information systems and services.

1.4. CURRENT STATUS OF GAMBIA'S CYBER SECURITY

The Gambia Government is aware of the global danger pose by cyber security threats to the integrity, security and privacy of information worldwide. In order to ensure safety and ensure protection of citizens from ICT based threats, every country shall have to protect its cyber-space.

To be able to fully realize the cyber security strategic objectives, there is the need for a strong institutional framework to harmonize and coordinate cyber security 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.

Currently, The Government of The Gambia has undertaken important steps in this direction. It has taken 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 Cyber security policy & strategy and strategic Action plans, Institutional Governance framework, Cybercrime Bill 2019 among others. The Cyber security strategy and Cybercrime Bill 2019 are yet to be enacted into law but expected to be achieved sooner than later.

The Gambia Telecommunications Act 2009 is general in scope but comprehensive; however the Act did was silent on substantive and procedural laws on cybercrime. This gap has now been addressed by the new draft cybercrime bill 2019. The adoption of national cybersecurity standards is other issue to be addressed. The use of standards as a measure of best practice is non-existent in some sectors of government. The lack of which have resulted to inconsistencies in information security assurance practices in both public and private sectors.

The draft National cybersecurity strategy provides for establishment of institutional frameworks such as The Gambia Information Communication Technology Agency (GICTA), National Cybersecurity Coordination Directorate (NCCD), Gambia Computer Security Incident Team (GM-CSIRT) and National Cybersecurity Committee/Commission (NCSC). All the above institutions would help protect critical infrastructure such as the National Backbone, National Data Center (NDC), SIXP (ISPs last mile networks), e-Government systems, Energy Infrastructure, Banking and Finance systems etc. This infrastructure needs to be highly protected both logically and physically.

In addition, Government promotes initiatives to build Cyber Security Capacity and to improve its capability. This also requires development and implementation of education and training programs, cybersecurity policy and strategy including collaboration and partnership with international partners to

ensure knowledge and skills transfer. Certainly, these initiatives are remarkable; however, there are still areas that require improved skills in order to meet the needs of all public and private sector stakeholders.

It is also important to establish a cyber-security culture and increase awareness among citizens as majority of public sector employees have low level of cybersecurity threat awareness. Although, the private sector operators and financial institutions have taken initiatives to address cyber threats. Generally there is still low-level cyber threat awareness at national and societal levels.

1.5. GUIDING PRINCIPLES

In order to align strategic objectives with current government efforts and international best practices, the development of the National Cyber Security Policy of The Gambia followed these guiding principles:

- **National Leadership** – The scale and complexity of cyber security requires strong national leadership and support;
- **Roles & Responsibilities** – All ICT users including government, businesses and citizenry should take reasonable steps 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 cyber security across government and the private sector is essential and crucial;
- **Risk-Based Management** – There is no such thing as absolute cyber security as security is a process in its own right. The Gambia must therefore apply a risk-based approach to assessing, prioritizing and resourcing cyber security activities.
- **Gambian Values** – The Gambia pursues cyber security policies that protect the Gambian society, the economy and the overall national vision.
- **International Cooperation** – The cross-border nature of threats makes it essential to promote international cooperation. The Gambia supports and will actively contributes to the international cyber security activity.

2. THE NATIONAL CYBER SECURITY POLICY

The Gambia National Cyber Security Policy establishes an environment that provides trust and confidence in the use of ICT facilities as well as ensures that Gambia is able to independently protect its interests and enforce national security. This policy shall guarantee the confidentiality, integrity and availability of information assets and classified information of Government, Businesses and individuals.

2.1 VISION

The vision is to develop cybersecurity policy that secures the Gambia's cyberspace in general.

2.2 MISSION

To determine, identify, analyze and address the immediate cyber security threats against people, entities, and critical national infrastructure of The Gambia. Provide adequate protection for critical national infrastructure, Information systems, Internet services and end users) to ensure The Gambia Cyber Space remain secure and resilient".

2.3. STRATEGIC OBJECTIVES

2.3.1 Objectives

For the goals set to materialize, the Government seeks to achieve the following five (5) policy objectives:

Objective 1	Objective 2	Objective 3	Objective 4	Objective 5
Cybersecurity Governance (Policy and Strategy)	Cyber Culture and Society	Cybersecurity Education, Training and Skills	Legal and Regulatory Framework	Standards, Organization, and Technologies

2.3.2 Strategic Goals

- **Strengthen Legal and Regulatory Frameworks** as well as promote compliance with appropriate technical and security standards
- **Promote awareness, training and education** in all sectors and levels in order to build a culture of security within country.
- **Establish an Institutional Framework** to foster cyber-security coordination
- **Build Cyber Security Capabilities** for prevention, protection, detection, and response to cyber security incidents and threats.
- **Ensure the Protection of Information Systems** in particular critical, information, infrastructure and services
- **Foster National and International Cooperation** in the field of cyber security.

2.4 POLICY SCOPE

This policy covers cybersecurity governance, legal measures, Law enforcement, national security and critical national infrastructure protection, awareness campaign, education and training to standardization.

2.4.1 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

2.4.2 Components of The Gambia's Cyberspace:

The country's cyberspace components 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 data centre • Food services • 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 cyber security initiatives and promote effective cooperation between public and private sectors. In order to sustain the gains from any such initiatives, a National Cybersecurity Coordination Directorate (NCCD) will be established under GICTA for formal coordination and information sharing.

3.2 Legislative and Regulatory Frameworks

MOICI and relevant stakeholders will collaborate with the Ministry of Justice to setup and ensure regular review process and enhancement of Gambia's cyber space legislation for purposes of addressing the dynamic nature of cyber security threats.

In order to empower national law enforcement agencies to properly prosecute cybercrimes, government will establish a sustainable capacity building programs to acquire new skills and effective ways of enforcing cyber laws. Government will further ensure that all applicable local legislation is complementary and in compliance with regional, international treaties, and conventions.

3.3 Cyber Security Technology Frameworks

Uniform policy measures will be put in place to develop a national cyber security technology framework that specifies Cyber Security requirement, controls and baselines for CNII elements. This will be followed by mechanism to implement and evaluate /Certification program for cyber security products and systems.

3.4 Security Culture and Capacity Building

GoTG will invest resources needed to develop, foster and maintain a national culture of security. As part of the process of development of culture on cyber security, government will support the standardization and coordination of cyber security awareness and education programmes across all elements of the Cyber space. The national awareness shall include civil society and national coordinating agencies.

Government will also establish an effective mechanism for cyber security 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 Cyber space to a level commensurate with the risk, government will formalize the coordination and prioritization of cyber security research and development initiatives. It will further enlarge and strengthen the cyber security research community.

Strategic research and development will be encouraged by promoting the development and commercialization of intellectual properties, technologies and innovations through focused research and development. Government will put in place programmes to promote the growth of cyber security industry in the country.

3.6 Compliance and Enforcement

In order to ensure compliance and enforcement, unified policy measures and mechanism will be put in place to standardize cyber security systems across all elements of Gambia's Cyber space. Government will also strengthen the monitoring and enforcement of standards and develop a standard cyber security risk assessment framework.

3.7 Cyber Security Emergency Readiness

To ensure cyber security emergency readiness, GoTG together with all stakeholders will develop effective Cyber Security incident reporting and Crisis management mechanism. This will include among others the development and strengthening of the Gambia Computer Incidence Response Team (GM-CSIRT) and sector focal points or CERTs in the dissemination of vulnerability notices and threat warnings in a timely manner.

Government will also ensure development of a standard business continuity and recovery management framework (BCP). The government will further encourage all elements of the Cyber Space to monitor Cyber Security events and implement or perform periodic vulnerability assessment programs.

3.8 International Cooperation

Policy measures will be put in place to encourage active participation of The Gambia in all relevant international Cyber Security organizations, panels and multi-national agencies.

Government will make every effort to promote active participation in all relevant international Cyber Security activities by hosting annual International Cyber Security Conference and national periodic cybersecurity workshops and seminars.

4.0 KEY POLICY DIMENSIONS

4.1 POLICY DIMENSION 1 – CYBER SECURITY CAPABILITIES

Objective: Build cyber security 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 cyber security threats and will play a leading role in managing incident response or crisis situation. GM- CSIRT operational capabilities in terms capacity building, and other vital technology resource well will strengthened.

II) Develop National Cyber Contingency Plan:

A National Cyber Security 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 cyber-security crisis.

III) Establish Cyber Security Capabilities within Institutions:

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

4.2 POLICY DIMENSION 2 – INSTITUTIONAL FRAMEWORK FOR CYBERSECURITY

Objective: To build cyber security capabilities and secure national information assets requires a sound governance structure for effective coordination of national cyber security initiatives.

4.2.1 Measures

I) The complexity of cyber security threats is such that the need for strong institutional framework to coordinate cyber security 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 Cyber Security Coordination Directorate within GICTA to be responsible for the development, implementation and coordination of the national cyber security initiatives. However in the interest of international good practice and depending on level of national cyber threat profile in scope and sophistication, a national Cyber Security Agency or Authority shall be establish to effectively tackle the growing Cyber security demands of the country.

II) Establish a National Cyber Security Advisory Board;

In order to establish strong cyber-security governance framework, the GoTG shall put in place a National Cyber Security Commission (NCSC). This commission shall provide coordination and strategic guidance on matters related to National Cyber Security.

The composition of the Commission shall be multi-sectoral; involving public, private and civil society stakeholders relevant to cyber security.

4.3 POLICY DIMENSION 3 – CYBER SECURITY 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 Measure

I) strengthen the legal and regulatory framework;

There is a need to enhance the current legal and regulatory framework to facilitate the enforcement of cyber security 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 cyber security 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 cyber security 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 standards and guidelines in collaboration with Gambia Standards Bureau and benchmarked with international standards such as (ISO/IEC 27001/002, ISO/IEC9000, ISO14000, ISO/IEC27037) or UK-ACPO Best Practice Guidelines for digital Forensics Investigation among host of other open standards. The public and private sector stakeholders shall adopt unified and consistent cyber security standards.

4.4 POLICY DIMENSION 4 – CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Objective: To protect National Critical Information Infrastructure against cyber threats and related cyber-crimes to ensure Confidentiality, Integrity and Availability.

4.4.1 Measures

I) Protect National Critical Information Infrastructure;

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

In collaboration with the Gambia ICT Agency (GICTA) and PURA, NCCD as well as the private sectors relevant to cyber security shall develop the CII Information Protection law, CII regulations, and compliance and protection plan. CII regulation shall address, but not limited to CII procedures manuals, access control, business continuity and contingency plan, physical and logical protection.

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 cyber security 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 cyber security related issues.

4.5 POLICY DIMENSION 5 – GOVERNMENT CYBER SECURITY ENHANCEMENT PROGRAMS

Objective: To safeguard Government information systems, services and critical infrastructure against cyber-attacks.

4.5.1 Measures

I) Information Security Assurance or Compliance;

The NCCD and GM-CSIRT in charge of Cyber Security 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). They shall equally seek support from the NCCD - GM-CSIRT in charge of cyber security.

II) Establish security classification for systems, applications and services

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

III) 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 certificate. 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 system as well as other sectors.

4.6 POLICY DIMENSION 6 – CYBER SECURITY CAPACITY BUILDING AND AWARENESS

Objectives:

- To build cyber security prevention and response capabilities;
- To create cyber security awareness for Gambian citizens.

4.6.1 Measures

I) Cyber Security Capacity Development

Cyber security 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 cyber security 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 cyber security will be created through capacity building, skills development and continuous professional training and development.

II) Develop a National Cyber Security Awareness Program

It is important that Gambian citizens using or operating information assets understand the threats and risks in cyber space. GM-CSIRT shall develop a cyber-security awareness program for institutions and individuals as well as encourage ownership. GM-CSIRT will coordinate and collaborate with cyber security alliance Gambia and other civil society organization for the advocacy campaign.

4.7 POLICY DIMENSION 7 – BUILDING A CYBER SECURITY INDUSTRY

Objective: Develop a stronger cyber security industry to ensure a resilient Gambian cyber space.

4.7.1 Measures

I) Foster Innovation through Research and Development

In cooperation with the University and the industry, a Cyber Security 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 cyber security industry, the products and services resulting from cyber security 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 cyber security industry development. To develop a stronger cyber security sector or industry, a public private partnership shall be established to develop cyber security services, skills and expertise that respond to cyber security objectives. This will enhance Gambia's capacity to provide services and skills inside and outside of the country in the cyber security field.

4.8 POLICY DIMENSION 8 – INTERNATIONAL COOPERATION

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

4.8.1 Measure

I) Promote and Strengthen National and International Collaboration;

Before engaging in cooperation and information sharing with partners, it is important to understand and respond to a constantly changing threat environment. International investigations depend on reliable means of cooperation and effective harmonization of laws.

National Cyber Security Coordination Directorate through MOICI 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 cyber security to enhance capabilities.

5.0 INSTITUTIONAL FRAMEWORK

5.1. PROPOSED INSTITUTIONAL FRAMEWORK FOR IMPLEMENTATION

Securing Gambia's national information assets requires an adequate and comprehensive governance structure for focus and coordination of national

cyber security initiatives. It is therefore necessary to establish an efficient coordination mechanism for effective cyber security and resilience.

The cyber-security implementation framework is composed of the Gambia ICT Agency (GICTA), National Cybersecurity Coordination Directorate (NCCD), Gambia Computer Security Incident Response Team (GM-CSIRT), National Cyber Security Commission (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 INFORMATION COMMUNICATIONS AND INFRASTRUCTURE

This Ministry is the overall national authority responsible of Cyber Security 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

5.2.3 NATIONAL CYBER SECURITY COORDINATION DIRECTORATE (NCCD)

This directorate shall be established under GICTA to organize governance and implementation of the Cyber security strategy. The NCCD shall advise the permanent secretary MOICI 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 cyber security Commission to jointly coordinate the implementation of the strategy.

5.2.4 THE NATIONAL CYBER SECURITY COMMSSION (NCSC)

The National Cyber Security Commission shall be established to provide leadership, oversight and guidance on implementation and development of national cyber security strategy and reports to MOICI. It is critically important that NCSC is inclusive of major stakeholders. Composition of the NCSC shall be reviewed on an annual basis, to ensure members of the commission are the most relevant and active stakeholders on cyber security.

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

The GM-CSIRT is responsible for planning, coordination and implementation of national cyber security initiatives. It shall ensure institutional conformance to information security standards, guidelines and best practices necessary to secure Gambia's cyber space. It will act as the governmental and national operational cybersecurity Centre. GM-CSIRT reports to PURA, MOICI and NCCD. It shall conduct cyber security audits, assessments and readiness exercises/drills for government institutions and develop security standards and best practices for The Gambia in general.

GM-CSIRT shall also conduct research on technical issues, support awareness campaigns and provide cyber-security training programs. GM-CSIRT will operate and maintains national cyber security infrastructure and systems and provides technical support to institutional cyber-security units or sector CERTs. It will be responsible for developing necessary expertise and conducting research and development in cyber security and further promote national awareness and coordinates cyber-security workforce development.

Furthermore, GM-CSIRT shall represent Gambia on international forums on issues of cyber security. It will also coordinate and support Government Ministries, Agencies and Private sector institutions to develop cyber security capabilities and implement this policy.

6.0 FINANCIAL AND LEGAL IMPLICATIONS

6.1. FINANCIAL IMPLICATIONS

The National Cyber Security 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. To establish and operationalize the Gambia Cyber Security Coordination Directorate (NCCD for example among host of others, will attract financial resources. The NCCD will spearhead the implementation of this policy and shall be answerable to GICTA. The NCCD will have the responsibility to define the short and long-term strategic plan and budget.

. 6.2. LEGAL IMPLICATIONS

The approval of this policy may require Act of parliament establishing cyber security regulation with its functions clearly defined. This will be followed by review of existing legal framework to ensure that all applicable national legislations incorporate cyber security provisions, to follow the normal law reform process and procedure as well as consultations.