MINISTRY OF INFORMATION AND COMMUNICATIONS

GOVERNMENT OF SIERRA LEONE

NATIONAL CYBERSECURITY POLICY

March 2021

Table of Contents

1. EXECUTIVE SUMMARY 1
2. BACKGROUND 3
2.1. Challenges and Developments with a focus on the Policy 3
2.1.1. Global Activities on Cybersecurity 3
2.1.2. Regional Initiatives 3
2.1.3. Local Initiatives 4
2.1.4. Need For Policy Update 4
3. NATIONAL CYBERSECURITY POLICY 5
3.1. Introduction 5
3.2. Vision and Mission 5
3.2.1. Vision 5
3.2.2. Mission 6
3.3. Policy Scope 6
3.4. Policy Context 6
3.5. Policy Measures 7
3.5.1. Legal Measures 7
3.5.2. Technical Measures 7
3.5.3. Organisational Measures 8
3.5.4. Capacity Building Measures 9
3.5.5. Cooperation Measures 9
3.6. Operationalisation of the Policy 9
4. NATIONAL CYBERSECURITY STRATEGY 10
5. INSTITUTIONAL FRAMEWORK 10
5.1. National Cybersecurity Advisory Council (NCSC) 10
5.2. National Cyber Security Technical Working Group (NCTWG) 10
5.3. National Cyber Security Centre/Authority 10
6. FUNDING CYBERSECURITY 11
7. ACRONYMS 12

1. EXECUTIVE SUMMARY

In the digital future, cybersecurity remains a critical success factor for every country. Failure to address potential cybersecurity challenges will result in a catastrophic digital transformation.

The Government of Sierra Leone (GoSL), in its bid to transform Sierra Leone through its digital transformation roadmap, viewed cybersecurity as a critical element of the entire digital transformation process. Accordingly, the Government is upgrading the 2016 National Cybersecurity Policy to ensure we are on the right path to succeed in our digital transformation agenda. The Policy is being updated to meet the emerging challenges of Sierra Leone's cybersecurity landscape.

The Policy document has five pillars in line with the ITU model as prescribed by the Global Cybersecurity Agenda as follows:

1. **Legal Policy Pillar:** This pillar focuses on legal issues needed to be addressed to ensure that cybersecurity in Sierra Leone is fully addressed.
2. **Technical Policy Pillar:** This pillar focuses on the Government's commitment to establishing technical operations to address cybersecurity challenges such as incident handling, forensics, and critical information infrastructure protection.
3. **Organisation Policy Pillar:** This pillar focuses on the Government's commitment to setting up an institutional arrangement to ensure the effectiveness of the implementation of cybersecurity initiatives in Sierra Leone.
4. **Capacity Building Pillar:** This pillar focuses on the Government's determination to create awareness amongst citizens and promote cybersecurity capacity, education, and training within the public sector, private sector, academia, and civil society.
5. **Cooperation Policy Pillar:** This policy pillar focuses on ensuring that Government works with the private sector through a Public-Private Partnership to address cybersecurity issues, harmonise Sierra Leone's legal test and fight against cybercrime with neighbouring countries in the sub-region and international partners.

The Government will set up a national agency to coordinate and manage national cybersecurity efforts and an oversight board and technical coordination body as the institutional framework for implementing this Policy. The Government will identify sources of revenue for addressing the cyber menace, starting with budgetary allocations, donor agency funding and taxes.

2. BACKGROUND

2.1. Challenges and Developments with a focus on the Policy

2.1.1. Global Activities on Cybersecurity

Some cybersecurity research firms report that cybersecurity incidents continue to rise, even though not at the same exponential rate[1]. Of greater importance is the complexity of these attacks. Cyber attackers continue to be a head of cybersecurity experts, launching complex attacks on networks. The report also indicates that the financial and technology sector is the most targeted globally. DOS/DDOS attacks are the leading global attack, and the United States is the source of most cyberattacks.

The average annual cost of cybercrime by attack type has increased across the board for all attack types. Cybersecurity challenges are currently a top priority agenda for many governments, which, if not addressed, will erode all gains made by digital transformation. The United Nations, through the ITU, is actively supporting the world through its Global Cybersecurity Agenda. The Global Cybersecurity Index offers the opportunity to measure the state of cyber readiness of countries. The World Bank also supports the fight against cybercrime through its Global Cybersecurity Capacity Building program. The Global Forum for Cyber Expertise also supports countries in the digital south with skill and capacity building. In the private sector, many companies are increasing budgets to fight cybercrime to keep risk at acceptable levels.

2.1.2. Regional Initiatives

Evidence suggests that the more the connectedness of countries, the higher the spate of cyberattacks. In Africa, South Africa appears to be most connected and leads with the highest number of attacks, about 20% of all attacks that come to Africa. Despite the prevalence of cyberattacks in the African cybersecurity landscape, the volume of attacks from the continent represents a small fraction of the global attack scenarios. To improve Africa's cybersecurity

[1] NTT Security Global Cyber Intelligence report for 2019

credentials, Africa Union developed and adopted Malabo AU Convention on Cybersecurity & Data Protection. This Convention provides guidelines and recommendations for all Member States to develop their cybersecurity strategies. The AU has also instituted several capacity-building programs on cybersecurity policy, technical and legal aspects, and the fight against cybercrime with its global partners. Moreover, it has set up a committee of experts to guide its cybersecurity programs.

2.1.3. Local Initiatives

In Sierra Leone, since the approval of the 2016 National Cybersecurity Policy by the Cabinet, several activities have taken place to give a clearer picture of the cybersecurity landscape. Firstly, in the same 2016, just after the approval of the Policy, a Cybersecurity Maturity Model (CMM) assessment was conducted by International Telecommunications Union (ITU); the Global Cyber Security Capacity Centre (GCSCC), which provides a good insight into the state of cybersecurity in Sierra Leone. Also, in 2019, the Ministry of Information and Communications conducted a National Cybersecurity Risk Assessment (NCRA) with support from the UK team of experts. This report provides an opportunity to identify some of the country's critical information infrastructure, including in-depth knowledge of the cyber threat landscape.

These activities, coupled with the development of Sierra Leone's National Digital Transformation Roadmap, lays a premium on the need for a risk-based cybersecurity strategy, including a necessity for protecting critical digital infrastructure and systems.

2.1.4. Need For Policy Update

Sierra Leone seeks to leapfrog into the digital world through its detailed Digital Transformation Roadmap, which will see several digital infrastructures developed. Moreover, for the citizens to fully participate in the Digital transformation, they must be protected in cyberspace. Hence, the need to create a security culture by creating awareness of the enormous threats that users of the Internet are exposed to needs to be addressed by a national cyber security policy. This awareness

activity will create a very conducive environment in the information economy where the people of Sierra Leone can generate wealth in peace without fear of harassment by cybercriminals and fraudsters.

The 2016 Policy was formulated as a document to address the issues mentioned above. However, this new policy document (an update of the 2016 Policy) will focus on addressing new gaps due to emerging cybersecurity threats that were not apparent in 2016 and incorporate aspects that were not captured in the 2016 Policy document.

3. NATIONAL CYBERSECURITY POLICY

3.1. Introduction

Sierra Leone's digital transformation roadmap requires securing cyberspace to ensure its people are free from attacks with devastating effects. Studies reveal that people with a cybersecurity culture achieved through awareness creation and capacity building are better positioned to handle cyber-attacks as and when they occur. Thus, the ability of Sierra Leoneans to identify and understand threats and manage them significantly reduces the number of actual attacks and enhances the continuous operation of the national infrastructure on which critical information is held in the nation's interest and security. Furthermore, the Government is aware that threats are not restricted only to public institutions but also to private operators who provide services to citizens. Therefore, tackling cybersecurity requires a public-private partnership approach.

3.2. Vision and Mission

3.2.1. Vision

The Government of Sierra Leone's vision for cybersecurity is for Sierra Leone to have a credible and secured cyberspace that protects national interests while empowering citizens with the freedom to use the Internet for socio-economic benefit safely.

3.2.2. Mission

Our mission is to deter cybercrimes, protect critical digital infrastructure, develop national cyber capabilities, empower the citizenry for a healthy digital way of life and strengthen cyber cooperation to support a robust digital economy.

3.3. Policy Scope

This Policy covers all aspects of cybersecurity and national response, including the fight against cybercrime, creating public awareness, investment in cyber education, scientific research, development of cyber laws and legal measures, national security, law enforcement, and protection of critical national information infrastructures.

3.4. Policy Context

The National Cybersecurity Policy (NCP) seeks to address the risks to the Critical National Information Infrastructure (CNII), which comprises the networked information systems of identified critical sectors to empower citizens with freedom to work within cyberspace to create worth at all times.

The Policy recognises the critical and highly interdependent nature of the CNII. It aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cybersecurity controls over vital assets. It is being designed to ensure that the citizens will have access at all times to the Internet and government services online. The CNII will be protected to a level commensurate to the risks faced and that no interruption (intentional or unintentional) prevents Internet use.

The Policy has been developed to facilitate Sierra Leone's move toward a knowledge-based economy. It will be based on several frameworks, including legislation and regulations, technology, public-private cooperation, institutional and international aspects.

The right of citizens to use the Internet and the guarantee of the freedom of expression form the foundation for the Policy's development. Promoting the well-being of citizens in cyberspace will also enable the socio-economic benefits to the country.

3.5. Policy Measures

The ITU global agenda provides a globally accepted approach to developing cybersecurity policy and strategy. It provides a structured approach to addressing cybersecurity concerns at the national level, which can easily be monitored as progress is made.

3.5.1. Legal Measures

To ensure that the legal foundation of the fight against cybercrime is sound and the rights of citizens are protected, Government will implement the following legal measures and frameworks:

1. The Government will conduct periodic reviews of Sierra Leone's cybersecurity and crime legislation through the Attorney General's Department and relevant agencies.
2. The Government will ensure that Sierra Leone's cybersecurity and crime Act is consistent and interoperable with regional and international laws, treaties, and conventions.
3. The Government will progressively build capacity in the justice sector, law enforcement and other relevant national institutions to enforce the cybersecurity and crime Act effectively.
4. Government with enact legislation to ensure that the rights of citizens to use the Internet to express themselves online in a responsible manner and protection of personal data are guaranteed.

3.5.2. Technical Measures

Vulnerabilities in hardware and software remain the main contributing factors for cyber-attacks as malicious attacks increase in complexity and sophistication. In this regard:

1. The Government will implement appropriate technical measures to ensure the security of Sierra Leone's digital ecosystem.
2. The Government will set up and operationalise:

    a. Sierra Leone's Computer Emergency Response Team (CERT) ecosystem
    b. Cybersecurity Risk Management Framework
    c. Standards for the Critical National Information Infrastructure (CNII) sectors
    d. Mechanisms for Cybersecurity Certification and Accreditations
    e. Child Online Protection (COP)

3. The Government will also implement a cyber defence strategy incorporating a national crises management plan.

3.5.3. Organisational Measures

Organisations and Governments recognise the importance of a multistakeholder approach to addressing cybercrime and cybersecurity challenges and acknowledge that institutional arrangements are prerequisites for the effective development of national cybersecurity. In this regard:

1. The Government will set up a national cybersecurity institutional framework that integrates governmental and non-governmental cybersecurity stakeholders and ensures accountability among them.
2. The Government will develop its cybersecurity strategy and set up a national agency responsible for its implementation and corresponding oversight bodies for coordinating cybersecurity governance, operations, and activities in Government and within the private sector.
3. The Government will set up regulatory mechanisms, legal authority, and guidelines to ensure national cybersecurity is effective and efficient.

3.5.4. Capacity Building Measures

To ensure the sustainable development of Sierra Leone's cybersecurity ecosystem, investment in capacity building is particularly important. To this end:

1. The Government will invest available resources to develop, foster and maintain a national cybersecurity culture.
2. The Government will embark on national cybersecurity awareness programmes and
    i. support the development and adoption of appropriate cybersecurity standards
    ii. invest in cybersecurity education across all levels to develop the country's cybersecurity human resource base
    iii. prioritise the development of the local cybersecurity industry and
    iv. invest in research and development towards self-reliance.

3.5.5. Cooperation Measures

Cybercrime and cybersecurity challenges are multidimensional and cross-border in nature. In this regard:

1. The Government will commit to partnerships and cooperation within Sierra Leone and through regional and international cooperation arrangements.
2. The Government will prioritise inter-ministerial engagements, inter-agency cooperation, and public-private partnerships in furtherance of Sierra Leone's cybersecurity cooperation agenda.
3. The Government will actively participate and contribute to international cooperation efforts towards addressing cybercrime and cybersecurity challenges.

3.6. Operationalisation of the Policy

This Policy shall be operationalised under the Ministry of Information and Communications' oversight by developing strategies, guidelines, and action plans through a multistakeholder approach to address the challenges to Sierra Leone cyberspace.

4. NATIONAL CYBERSECURITY STRATEGY

A strategic document shall be developed to implement the policy decision of the Government of Sierra Leone. The strategy shall have its critical goals as follows:

a) **C**reate institutional, legal, and regulatory frameworks for effective governance
b) Promote public education and awareness, online child protection, rights and privacy of citizens
c) Develop cyber capabilities to support national security objectives, protect critical digital infrastructure through response readiness and
d) Strengthen national, regional, and international cooperation.

The Government will implement special initiatives and actions under the strategy.

5. INSTITUTIONAL FRAMEWORK

5.1. National Cybersecurity Advisory Council (NCSC)

The National Cybersecurity Advisory Council has been created to act as the advisory board to the National Cybersecurity Centre. The Council shall provide strategic leadership, oversight, and guidance on implementing and developing national cyber security initiatives.

5.2. National Cyber Security Technical Working Group (NCTWG)

The National Cybersecurity Technical Working Group will be created as the technical group that will take operational decisions on implementing cybersecurity interventions. It comprises heads of institutions actively involved in implementing different aspects of cybersecurity interventions.

5.3. National Cyber Security Centre/Authority

In line with global best practices, a National Cybersecurity Centre will be established to coordinate all cybersecurity activities in Sierra Leone. It will, among others, be responsible for developing

regulations and enforcing cybersecurity standards. It will also undertake operational activities at the national level, including management of Critical National Information Infrastructure (CNII) protection and the Computer Security Incident Response Team (CSIRT).

6. FUNDING CYBERSECURITY

The National Cybersecurity Strategy will identify several interventions that the Government plans to use in implementing the Policy. In the short term, the Government will allocate a budget while seeking grants from donor agencies and international partners to implement the special actions and initiatives.

7. ACRONYMS

Acronym	Interpretation
AU	Africa Union
CMM	Cybersecurity Maturity Model
CERT	Computer Emergency Response Team
GCSCC	Global Cyber Security Capacity Centre
CIIMP	Critical Information Infrastructure Measurable Programme
CIIP	Critical Information Infrastructure Protection
CII	Critical Information Infrastructure
ECOWAS	Economic Community of West Africa States
GoSL	Government of Sierra Leone
MIC	Ministry of Information & Communications
ITU	International Telecommunications Union
ICT	Information & Communication Technology
IT	Information Technology
MEST	Ministry of Education Science and Technology
MoFED	Ministry of Finance and Economic Development
MOFAIC	Ministry of Foreign Affairs and International Cooperation
NATO	North Atlantic Treaty Organisation NCIRT National Cyber Incidence Response Team
NCIIPP	National Critical Information Infrastructure Protection Plan
NCSC	National Cybersecurity Council
NCSP	National Cybersecurity Policy
NCSS	National Cybersecurity Strategy
NCSTC	National Cyber Security Technical Committee
NCSTWG	National Cybersecurity Technical Working Group
NCRA	National Cybersecurity Risk Assessment
NDTR	National Digital Transformation Roadmap
ONS	Office of National Security
OECD	Organisation for Economic Cooperation and Development
OSCE	Organisation for Security and Cooperation Europe
PPP	Public-Private Partnership
UN	United Nation