REPUBLIC OF SEYCHELLES

THE OFFICE OF THE PRESIDENT

DEPARTMENT INFORMATION AND COMMUNICATIONS TECHNOLOGY

NATIONAL CYBER SECURITY POLICY

2019

TABLE OF CONTENTS

1. Introduction

1.1 Background

The purpose of this policy is to set a vision for the future of cybersecurity in Seychelles to be achieved over the course of the next 5 years. It seeks to provide a framework for effective implementation of security principles, which may be evaluated against evolving security standards, allowing government officials to reasonably monitor the balance of security risks and allocated resources to mitigate them. This policy aims not to focus only on preventing attacks, but to equip organisations to respond to the growing likelihood that cyber defences will be breached, that data will be illicitly removed and that control of systems will be undermined.

ICTs are at the very core of the delivery government services, business services and civil society operations. As such, the need to have a national policy framework for addressing cybersecurity is important for the continued development of the Seychelles. Various regional and international level organisations are also involved in addressing the concerns and challenges presented by cybersecurity.

Cybersecurity has been identified during the 1st phase of the World Summit on the Information Society (WSIS) process as one of the critical issues for African development. The WSIS Action Plan recommends “co-operation among the governments at the United Nations and with all stakeholders at other appropriate forums to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues”.

The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the WSIS in two phases. The objective of the first phase in Geneva was to develop and foster a clear statement of political will and take concrete steps to establish foundation for an information society for all, reflecting all the different interests at stake. The objective of the second phase in Tunis was to put the Geneva Plan of Action into motion as well as to find solutions and reach agreements in the field of Internet governance, financing mechanisms, and follow up and implementation of the

Geneva and Tunis documents. The WSIS Action line C5 identifies the need to build confidence and security in the use of ICT's. The Tunis World Summit on the Information Society mandated the International Telecommunication Union (ITU) to assist in further developing the Global Cyber security Agenda (GCA), a High-Level Experts Group (HLEG) on Cyber security was established to support the Secretary General to assist countries to develop Cybersecurity intervention identified the following key pillars: organizational structures, legal, technical and procedural measures, international collaboration, and national partnership of stakeholders.

The ITU has sought to address the concerns and challenges facing Cybersecurity through various instruments. In its Cyber Security Agenda Framework (launched in 2007), the ITU highlights that cybersecurity and cyberspace are the most critical concerns of our information age. Criminals are on the prowl to prey on the unwary and use their technical skills to break into networks not only for financial gain but also to collect information, invade privacy, steal identities, sow hatred and, worst of all, pander to the nefarious habits of paedophiles.

In the world of ICT, there has been a growing trend that attackers are able to deeply penetrate and remain hidden inside computer networks, despite best efforts to keep them out – so vigilance and risk-led deployment of limited security resources are essential to the effective implementation of a cybersecurity policy. A cybersecurity policy needs to address not only the technical aspects of security, but should fully engage the process of designing security into processes and the human interaction and usage of ICT.

Global efforts have been made to harmonise policy and legal frameworks. In particular, the African Union Commission and the United Nations Economic Commission for Africa developed a convention on cybersecurity, which underwent a series of reviews by the regional economic communities, and was endorsed by the African Union Ordinary Conference in Charge of Communication and Information Technologies in September 2012, and which was adopted by the African Union Heads of State and Governments Summit in June 2014 in Malabo.

Recognizing the multifaceted nature of cybersecurity issues and the factors that impact on them, the Government is conscious that the successful implementation of this policy and achievement of its objectives is through partnership with the private sector and civil society. Consequently, the participation and involvement of all key relevant stakeholders from Government, civil society and

private sector is crucial.

In addition, the Government will continue to develop the necessary capacity and instruments, such as cybersecurity indicators, to monitor the impact of the policies on social and economic development.

Mindful of the fact that the cybersecurity itself is one of the most dynamic areas, necessary mechanisms will have to be put in place to ensure that the policies are reviewed from time to time. Enhancing of knowledge and information flows is one of the effective tools that would be used to stimulate innovation and facilitate fine-tuning of the policies for the maximum impact and responsiveness to changing technological and competitive conditions.

In developing this policy, Seychelles government seeks to provide a secure, safe and resilient cyber space for all ICT users.

1.2 Vision

For Seychelles to use a secure, resilient and trusted cyberspace, which contributes to national economic and social prosperity.

1.3 Mission

The Mission of this policy is to ensure and create confidence in the use of ICT within Seychelles to the highest attainable levels by ensuring security in electronic communications and transactions.

2. Guiding Principles

This cybersecurity policy is based on the following guiding principles:

2.1 Shared Responsibilities & Subsidiarity: All users, in enjoying the benefits of ICT, should take reasonable steps to secure their own systems, exercise care in the communication and storage of sensitive information and have an obligation to respect the information and systems of other users.

2.2 Cooperation: In light of these shared responsibilities, a partnership approach to cyber security across all Government Ministries, Departments and Agencies, the private sector, Civil Society and the broader Seychelles community is essential. Given the transnational nature of the Internet, in which effective cybersecurity also requires coordinated global action, Seychelles must also adopt an active, multi-layered approach to international engagement on cybersecurity.

2.3 Risk-Based Approach & Proportionality: In a globalised world where all Internet-connected systems are potentially vulnerable and where cyber-attacks are difficult to detect, there is no such thing as absolute cyber security. Seychelles must therefore apply a risk-based approach to assessing, prioritising and resourcing cyber security activities. The focus being on cyber resilience.

2.4 Protecting Seychelles Fundamental Values: Seychelles must pursue cyber security policies that enhance individual and collective security while preserving Seychelles' right to privacy, access to information and other fundamental values and freedoms enshrined in its constitution.

3. Policy Objectives

3.1 ICT Infrastructure:

Implement measures to protect Seychelles' cyberspace and ICT infrastructure, to promote resilience to cyber-attacks and to respond to threats.

3.2 Legal and Regulatory Framework on Cybersecurity:

Develop a comprehensive, flexible and robust legal and regulatory framework to address issues of cybersecurity and combat cybercrime.

3.3 Organisational Structures & Governance:

Ensure that Seychelles has the right organizational structure, and processes in place to ensure that organisations can work effectively together and ensure that the country is as resilient as possible vis-à-vis cyber threats.

3.4 Human Resource Development & Education:

Ensure that Seychelles has the right people, with the right skills and knowledge to ensure that it has a credible cybersecurity capability to ensure resilience vis-à-vis cyber threats.

3.5 International Collaboration:

Establish effective mechanisms for international co-operation to enhance and promote Seychelles' cybersecurity efforts.

4. Policy Statements

4.1 ICT Infrastructure

(i) Develop and implement a Cyber Resilience programme. The programme will be based on risk assessment and Business Continuity Management (BCM), using internationally recognised security standards to:

a. Identify all relevant infrastructure, including the Critical Communication and Critical Information Infrastructure (CII);
b. Assess and provide the necessary resources to implement and operate resilient ICT infrastructure and its management in organisations;
c. Monitor, document and address incidents.

(ii) Provision of a unique digital identity of every Seychellois citizen based on a National Public Key Infrastructure (PKI);

(iii) Promote the wide use of Digital Signature generated using the National PKI for electronic transactions in Seychelles.

4.2 Legal and Regulatory Framework on Cyber-security

(i) To enhance public confidence, privacy and trust in the use of ICT services, systems and access to information.

(ii) Formulate legislation to combat cybercrime. The legislation will:

a. Align with international best practice and Seychelles obligations under international law;
b. Ensure evidence of crimes under the legislation can be collected, retained and admitted in legal proceedings;
c. Enable formal and informal international cooperation;
d. Balance protection of rights and freedoms under the Constitution.

(iii) Enhance cybersecurity law enforcement capability.

Law enforcement agencies in Seychelles will enhance its facilities to prevent, investigate and prosecute offences under the Cybercrime and related laws. This will include:

a. Capacity building in the implementation of new legislations;
b. Review and enhance powers of law enforcement agencies in this area;
c. Putting in place new facilities (e.g. cyber-forensic lab) to support implementation.

(iv) Implement legislation for data protection. The legislation will:.

a. Regulate the collection, use, disclosure, processing, storage of personal information (including sensitive personal information);
b. Regulate how and when data is to be destroyed;
c. Offer mechanisms for complaints about the handling of data;
d. Include offences criminalising falsification and certain dealings;
e. Align with international best practices in relation to data protection;
f. Establish a body with functions and powers under the Act.

4.3 Organisational Structures & Governance

(i) To establish a national level governance structure for coordinating work of multiple stakeholder organisations addressing cybersecurity issues. The governance structure will define the roles, responsibilities and accountability of these organisations.

(ii) To establish a national Computer Emergency Response Team (CERT). This will be Government in conjunction with the private sector and civil society. The CERT will not only be a specialist group of people who respond to incidents after they have happened, but will take the lead role in strengthening preventative security by proactive means.

(iii) Government will establish a dedicated Cybersecurity Security Unit that will be responsible for cybersecurity in the Civil Service.

(iv) To promote the adoption of international best practice cybersecurity and information security processes and standards in as many organisations as possible.

4.4 Human Resource Development & Education

(i) To increase the number of information security professionals in the country. This will include:

a. Sponsoring or funding training programmes for government officials to become certified information security professionals;

b. Establishing a certification regime for training programmes to become information security professionals.

(ii) Put in place a cybercrime awareness campaign. This will be both for the general public and for specific target groups with specific awareness requirements such as government officials, civil society, children & parents and SMEs:

a. Guidelines about how to mitigate against cyber threats;
b. Encourage the use of available technical tools that improve security online;
c. Use of mass media for sensitisation;
d. Making information available online.

4.5 International Collaboration

(i) To sstablish international relationships targeting bilateral, multinational or regional cybersecurity initiatives. This includes:

a. Membership of international organisations such as FIRST (Forum for Incident Response and Security Teams), IMPACT (International Multilateral Partnership Against Cyber Threats) and others addressing cybersecurity;
b. Continuing engagement in regional and international bodies to, facilitate the development of international initiatives, the sharing of information about cybercrime, and criminal prosecution of offences;
c. The National CERT seeking to establish relationships with CERTs in other countries to support its operation.

5. Policy Implementation & Monitoring

The Department of ICT (DICT) will be the Government body responsible for overseeing the application of the policy and its implementation. The specific actions, initiatives and projects required for the implementation of this policy are specified in the National

Cybersecurity Strategy. These are included in the action plan of the cybersecurity strategy document. It is to be noted that the strategic objectives of the cybersecurity strategy are aligned to the policy objectives and statements in the cybersecurity policy document.

Internationally recognized cybersecurity indicators will be used, as far as possible, to measure and monitor the impact of the policy. The use of recognized international indicators will also allow the benchmarking of the Seychelles cybersecurity posture with that of other countries. The key projects and initiatives identified in the National Cybersecurity Strategy are also incorporated in the DICT Strategy Plan and their implementation and outcomes are measured using the results based framework of the Performance Management & Evaluation (PM&E) of RBM (Results Based Management). In this framework the specified objectives and indicators are SMART and should allow objective measurement of the implementation of the projects or initiatives. The Department of ICT (DICT) will be the focal point for collating data and information for reporting on these indicators.