REPUBLIC OF SEYCHELLES

OFFICE OF THE PRESIDENT

DEPARTMENT OF ICT

NATIONAL CYBERSECURITY STRATEGY

2019 - 2024

TABLE OF CONTENTS

1. Introduction

The use of ICT and the internet now permeates the majority of sectors in the Seychellois society. The Seychelles is becoming increasingly dependent on ICT for running Government processes effectively and for maintaining productivity in all sectors of the economy. As such, the risks associated to cyber-attacks are also ever-growing, and threats from unknown sources are dynamic and constantly evolving. More frequently than ever before, reports on significant security incidents are being given prominence in the media, illustrating the need to have an effective and efficient strategy for operationalising the cybersecurity policy and management of cyber- security nationally.

ICT systems and networks form a vital part of the economy and society of a country. For this reason, they are generally regarded as critical information infrastructure (CII), as their disruption or destruction would have a serious impact on vital societal functions. CIIs are those systems that provide the resources upon which all the functions of society depend, such as telecommunications, transportation, energy, water supplies, healthcare, emergency services, service industries and financial services, as well as essential governmental functions. As a consequence, every single country that is connected to the internet has an interest in the implementation of capabilities to effectively and efficiently respond to cybersecurity incidents, and protect these essential functions from a national security perspective. The Cybersecurity Strategy aims to achieve this by implementing a series of projects and initiatives that will allow Seychelles to achieve this and also be as resilient as possible in relation to cyber-attacks.

Cyber-threats can come from anywhere in the world. As such, the development of dependable international corporations is also a cornerstone of the National Cybersecurity Strategy.

To implement the strategy is also recognised that this requires a multi-stakeholder approach and this is reflected in the proposed Governance structure for managing cybersecurity nationally.

1.2. Vision

For Seychelles to be resilient to cyber threats in order to continue leveraging ICT to contribute to national economic and social development.

1.3. Mission

To put in place a cybersecurity ecosystem nationally to enhance the resilience of the country to cyber threats.

1.4. Strategic Objectives/Goals

The Cybersecurity Strategic Plan is guided by the National Cybersecurity Policy. There are 5 areas addressed by the policy. The areas and their associated strategic objectives are:

1.4.1 Legal and Regulatory Framework on Cybersecurity: To develop a comprehensive, flexible and robust legal and regulatory framework to address issues of cybersecurity and combat cybercrime.

1.4.2 ICT Infrastructure: To implement measures to protect Seychelles' cyberspace and ICT infrastructure, to promote resilience to cyber-attacks and to respond to threats.

1.4.3 Oganisational 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.

1.4.4 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.

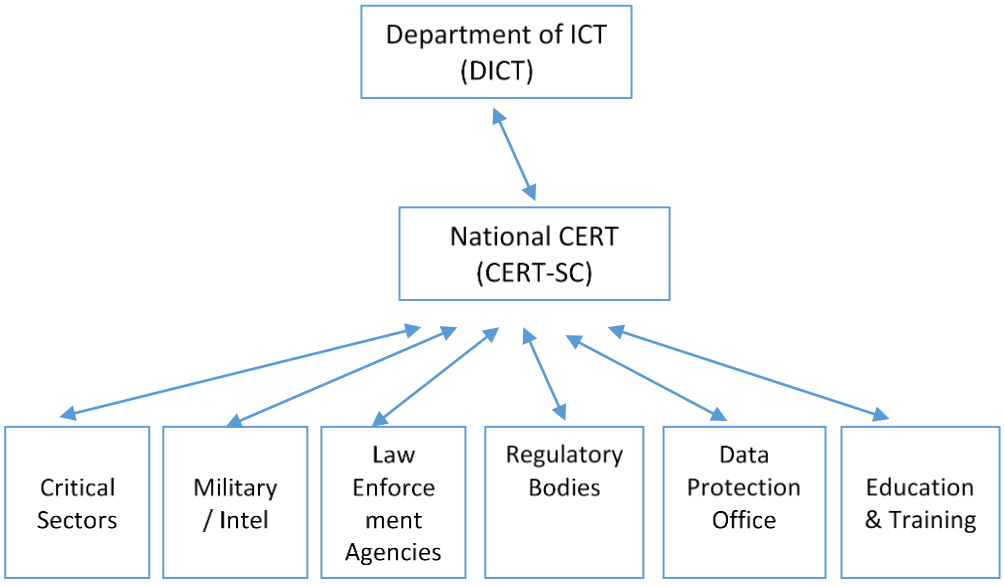
1.4.5 International Collaboration: Establish effective mechanisms for international co-operation to enhance and promote Seychelles' cybersecurity efforts.

2. Cybersecurity Management

In the Cybersecurity Policy under the policy statements relating to 'Organisational Structure & Governance' it is recognised that a national level governance structure needs to be established for coordinating work of multiple stakeholder organisations addressing cybersecurity issues. The governance structure also requires that the roles, responsibilities and accountability of these organisations to be clearly defined. As such, the following Governance structure and associated roles are proposed as part of the strategy.

2.1. Cybersecurity Governance Structure

To ensure effective protection of information infrastructure assets a collaborative working model is required that allows the formation of a close partnership between Government, corporate and the private sector. This partnership is required to allow for detection of cyber threats and coordinated response to address or mitigate them at a national level. This in turn should result in a more secure environment by allowing a wider range of stakeholders to properly address threats. To achieve this the following structure is proposed.



CERT-SC has to be setup and in line with international practice it is expected that it will be established under an appropriate legislation. It is proposed that the setting up of the CERT in this manner goes through the following phases:

- DICT assumes the responsibilities and functions of the CERT within its existing structure;
- CERT-SC is setup operationally as a separate structure (e.g. a section) within DICT;
- The legislation is formulated to create CERT-SC as a distinct body and the CERT-SC structure within DICT is made into this distinct body. All CERT functions are transferred from DICT to the CERT-SC body created under that legislation.

The proposed approach permits an optimised management of available resources in this area and a supportive framework for the development of capabilities locally to allow the implementation of a fully capable National CERT.

2.2. Roles of Stakeholders

The different stakeholders and their roles in the collaborative governance framework are given in the following table.

Stakeholders	Roles
Department of ICT (DICT)	DICT is the main project owner under the Cybersecurity Strategy Action Plan and is responsible for setting-up of the necessary legal framework for strategy implementation. It is also responsible for the implementation of information security standards and IT security best practice across the Government since it also contains the Cybersecurity Unit (CSU). The CSU will also constitute the Cyber-Defence Center for the Government Civil Service.
National CERT (CERT-SC)	This is the structure for coordinating information security issues nationally. The responsibilities of the National CERT will be: • To handle and coordinate the response to cybersecurity incidents. It is proposed that it establishes a cybersecurity coordination committee for this purpose which has membership from all key stakeholders; • To implement the outputs generated from the cybersecurity coordination committee; • Lead activities associated with developing and managing national (Critical Information Infrastructure Protection) CIIP efforts, including coordinating policy development, outreach and awareness, risk assessment and management efforts; and • To monitor and analyse the information security situation at national level; • To prevent occurrence and recurrence of cyber incidents by developing incentives for cybersecurity compliance and proactive actions;

	• To promote the adoption of best practices in information security and compliance.
Law Enforcement	Law Enforcement will be represented by the Police. Their roles will be to enable effective prevention, investigation, and prosecution of offences about cybercrime.
Military / Intelligence	Their role will be to advise and support efforts to protect Seychelles from directed threats and attacks. It is also to develop capabilities to respond to such threats and to gather signals intelligence.
Regulatory Bodies	The roles of the regulatory bodies will be to: • Establish, control, inspect and enforce regulations with regard to cybersecurity; • Encourage organisations to adopt security best practices and guidelines. Bodies covered by this might be the Central Bank of Seychelles, the FIU and other organisations with the responsibilities described.
Critical Sectors	The role of the critical sectors will be to facilitate identification, prioritization, assessment and protection of critical information infrastructure through information sharing and reporting. The critical sectors are those that are key to economic survival and functioning of the country. They the financial services, fisheries, tourism, ICT & Broadcasting, health, government services, public utilities, transport and logistics. The private sector is also to be represented in the associated different sectors identified. Some critical sectors (e.g. financial services) may also set up their own sector CERTs which will need to coordinate with the National CERT.
Data Protection Authorities	This body will act on data protection and privacy issues.
Academia / Education & Training	This is to constitute tertiary level institutions and their associated policy-making or funding bodies. Their roles are to: • Encourage Research & Development in the cybersecurity field to identify optimal solutions for Seychelles; • Develop educational and training programmes for developing cybersecurity professionals and students.

3. Cybersecurity Strategic Action Plan

The set of targeted projects and initiatives under each of the strategic goals are provided in the following table.

Strategic Goal 1: Develop a comprehensive, flexible and robust legal and regulatory framework to address issues of cybersecurity and combat cybercrime							
Objective	**Project / Initiative name**	**Description**	**Lead**	**Stakeholders**	**Priority**	**Start Date**	**End Date**
1. Put in place more effective legislation to combat cyber crime	Cyber Crimes Bill	The legislation will: • align with international best practice and Seychelles obligations under international law; • ensure evidence of crimes under the new legislation can be collected, retained and admitted in proceedings; • enable formal and informal international cooperation; • Balance protection of rights and freedoms under the Constitution.	DICT / AG's Office	POLICE, HOME AFFAIRS JUDICIARY CRITICAL SECTORS	High	2019	2020
	Cybercrime / Cybersecurity related legislation development training	To develop the capacity of officers involved in the formulation of cybersecurity related legislations.	HOME AFFAIRS / AG's Office	POLICE JUDICIARY DICT	Medium	2020	2022
	Alignment of local legislations to key regional & international conventions	A review of the different legal instruments in existence in Seychelles and to identify changes required to make them aligned with provisions of the AU Convention on Cyber Security & Personal Data Protection and the Budapest Convention. This is the process for the harmonisation of domestic laws with these conventions.	HOME AFFAIRS / DICT / AG's Office	POLICE JUDICIARY CRITICAL SECTORS MFA	Medium	2021	2024
2. Enhanced cybersecurity law enforcement capability	Police powers review	Undertake a detailed review of legislation and documents dealing with police powers, with a view to modernising powers for the digital age.	HOME AFFAIRS / POLICE	AG's Office JUDICIARY DICT	Medium	2020	2023
	Police & Prosecution training	Develop and deliver specific police and prosecutor training to allow more successful investigation and prosecution of cybercrimes.	POLICE / AG's Office	ANHRD JUDIICIARY	High	2020	2022
	Police facilities enhancement	Establish a specialist team with the required facilities and tools within the POLICE that have expertise in cybersecurity and cyber-forensics.	POLICE	HOME AFFAIRS DICT	High	2020	2021

3. Put into operation legislation for data protection	Data Protection Bill	The legislation will: • regulate the collection, use, disclosure, processing, storage of personal information (including sensitive personal information); • regulate how and when data is to be destroyed; • offer mechanisms for complaints about the handling of personal data; • align with international best practice in relation to data protection; and • establish or designate a body with functions and powers under the Act.	CBS / DICT	CIVIL SOCIETY JUDICIARY POLICE LOCAL IT SECTOR (THRU' SCCI) CBS FSA CRITICAL SECTORS DOI FTC	medium	2019	2020
	Implementing provisions of the Data Protection Bill	Establish the required structure prescribed by the bill after it has been enacted to allow the operationalization of the act.	DOI	ALL SECTORS	medium	2020	2021
Strategic Goal 2: Implement measures to protect Seychelles' cyberspace and ICT infrastructure, to promote resilience to cyber attacks and to respond to threats.							
Objective	**Project / Initiative name**	**Description**	**Lead**	**Stakeholders**	**Priority**	**Start Date**	**End Date**
1. Improve cyber-defence of critical information infrastructure nationally & reducing the impact of cyber-attacks.	Cyber resilience programme	Develop a permanently implemented cybersecurity resilience programme, using risk assessment and business continuity management tools. This will also include identification of the critical information infrastructure and the development of a Critical Information Infrastructure Protection (CIIP) framework and its implementation.	CERT-SC / DICT	MINISTRY OF FINANCE CRITICAL INFRASTRUCTURE OWNERS CRITICAL SECTORS	high	2020	2021
	Cyber Crisis Management Plan	To enable oganisations to prepare for responding to cybersecurity incidents and assess preparedness in responding to cyber-attacks.	CERT-SC / DICT	CRITICAL SECTORS MDAs TELCOS POLICE	medium	2021	2023

	Secure software development	To encourage the use of secure international best practise processes and security provisions for locally developed software.	DICT	SLA INDUSTRY SIB LOCAL IT COMPANIES	medium	2021	2024
	E-Government compliance	To ensure that all E-Government initiatives are compliant with international security best practices and have business continuity management catered for.	DICT / MDAs	IT COMPANIES	High	2020	2022
2. Improve the national ability to detect cyber threats & security breaches to prevent them and better able to disrupt attacks.	Cybersecurity drills & Testing of network security of organisations	To encourage organisations to periodically test and evaluate the adequacy and effectiveness of technical and operational measures of their IT systems and networks.	CERT-SC / DICT	CRITICAL SECTORS MDAs TELCOS	medium	2021	2024
	Adoption of minimum cybersecurity provisions in organisations	To formulate and promote the implementation of basic but essential cybersecurity measures in all organisations. The intention is to mitigate risks nationally from cyber threats.	DICT	PRIVATE SECTOR CIVIL SOCIETY INDIVIDUALS	medium	2021	2022
	Mandatory Information Security Auditing	To make mandatory information security audits in specific areas or organisations. This will be mandatory for MDAs.	DICT	MDAs CRITICAL SECTORS	High	2021	2024
Strategic Goal 3: 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.							
Objective	**Project / Initiative name**	**Description**	**Lead**	**Stakeholders**	**Priority**	**Start Date**	**End Date**
1.To address cybersecurity issues in Government in a systematic &	Cyber Security Unit (CSU)	The cybersecurity unit is to be part of DICT and is to separate the cybersecurity responsibility function from that of operation of the Government IT facilities.	DICT	SPECIALIST SECURITY SERVICE PROVIDERS	High	2019	2019

coordinated way		The CSU will be responsible for the implementation of information security standards and IT security best practice across the Government.		INTERNATIONAL STANDARDS ORGANISATIONS			
2. To enable national level coordination and collaboration in relation to addressing cybersecurity matters	CERT-SC establishment	The Department of ICT and key stakeholders from both private sector, civil society and Government will establish a National Computer Emergency Response Team (CERT-SC). As part of the CERT-SC governance structure there will also be the setting up of the National Cybersecurity Coordination Committee.	DICT	LAW ENFORCEMENT MILITARY REGULATORY BODIES CRITICAL SECTORS DATA PROTECTION OFFICE	High	2020	2021
3. To put in place best practice information security processes	International Standards for Information Security	To adopt the implementation of security standards such as ISO 27001. ISMS is to be implemented in MDAs that have mission critical information systems.	DICT/ SBS/ REGULATORS	MDAs CRITICAL SECTORS	High	2019	2020
4. To ensure that cybersecurity issues are addressed in organisations in a systematic and persistent manner.	Promote designation of a senior officer responsible for Information Security within the organisation	To promote the designation of a member of management or specialist in oragnisation (public & private) to be responsible for the implementation of cybersecurity initiatives.	DICT	ALL SECTORS	Medium	2020	2022
Strategic Goal 4: 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.							
Objective	**Project / Initiative name**	**Description**	**Lead**	**Stakeholders**	**Priority**	**Start Date**	**End Date**
1. To expand awareness of cybersecurity issues in society & hinder	Cybersecurity awareness campaigns	Conduct a public awareness campaign to promote the new laws about cyber crimes.and also sensitise members of the public to cyber	DICT	MEDIA MEDIA COMMISSION EDUCATION REGULATORS	High	2020	2024

the cyber threats		threats. This includes first line prevention and mitigation measures.					
	Cybersecurity Awareness & Education in the Government / Civil Service	To conduct cybersecurity sensitisation and training sessions throughout the civil service.	DICT	DPA TRAINING INSTITUTIONS	Medium	2021	2024
	Cybersecurity Training for SMEs	To have specific cybersecurity training programmes targeting local SMEs specifically. This is to promote the development a cybersecurity culture in SMEs.	ESA	DICT TRAINING INSTITUTION	Medium	2021	2024
	Cybersecurity Education	To incorporate aspects of cybersecurity awareness and knowledge in the curriculum at all levels of the education system.	MOE	CURRICULUM DEVELOPERS SITE	Medium	2020	2024
2. To develop local cybersecurity capability and deepen understanding of threats, vulnerabilities & risks in order to effectively mitigate against these.	Information Security professional development	Provide government support for initiatives to increase the number of information security professionals in Seychelles.	TEC / ANHRD	DICT MINISTRY OF EDUCATION TERTIARY EDUCATION INST PROFESSIONAL CENTERS	High	2021	2024
	Certification in security from recognised international organisations	To promote practising security professionals or IT professionals with security responsibilities to become certified by recognised international organisations in this field.	TEC	DICT TRAINING INSTITUTIONS SQA ANHRD	Medium	2021	2024

Strategic Goal 5: Establish effective mechanisms for international co-operation to enhance and promote Seychelles cybersecurity efforts.

Objective	Project / Initiative name	Description	Lead	Stakeholders	Priority	Start Date	End Date
1. To develop regional and International relationships for enhancing national cybersecurity	International membership	Identify and apply for membership of key international organisations related to cybersecurity.	DICT	MFA Ministry of Foreign Affairs) AG's Office	medium	2019	2021

capabilities and combating cybercrimes.							
	International cooperation	Support continuing engagement in regional and international bodies with cybersecurity agendas. In particular with COMESA, SADC, Commonwealth and AU	DICT	MFA Ministry of Foreign Affairs) AG's Office	medium	2020	2023
	CERT relationships	Establish good working relationships with other CERTS and relevant regional bodies.	DICT / CERT-SC	MFA LAW ENFORCEMENT AG's Office HOME AFFAIRS	high	2019	2021
	Attendance or Organisation of regional or international cybersecurity events	This is to foster networking with international partners, develop contacts and be exposed to the latest developments in this field.	DICT	LAW ENFORCEMENT MDAs	medium	2021	2024
2. To enhance the capability of local law enforcement agencies in dealing with cyber and related crimes	Partnerships with overseas law enforcement agencies	Establish specific relationships with law enforcement agencies (e.g. other POLICE forces) of friendly countries to provide specialist forensic support in areas where the local law enforcement agencies have deficiencies.	POLICE / FIU	MFA AG's Office DICT HOME AFFAIRS	High	2019	2021