REPUBLIC OF MAURITIUS

NATIONAL CYBER SECURITY STRATEGY

2014 - 2019

FOR A RESILIENT AND SECURE MAURITIUS
security
STELLA CLAVISQUE MARIS INDICI

The time has come for the protection mindset to be broadened – to embrace the broader concept of resilience ... The aim is to build a more resilient nation – one where all Mauritians are better able to adapt to change, where we can reduce exposure to risks, and where we are all better able to bounce back from disaster.

TABLE OF CONTENTS

Part 1

Part 2

Part 3

Part 4

List of Abbreviations

AML – Airports of Mauritius Limited
BOM – Bank of Mauritius
CEB – Central Electricity Board
CERT-MU – Computer Emergency Response Team of Mauritius
CIB – Central Informatics Bureau
CISD – Central Information Systems Division
CWA – Central Water Authority
DPO – Data Protection Office
FSC – Financial Services Commission
GOC – Government Online Centre
IBA – Independent Broadcasting Authority
ICTA – Information and Communications Technologies Authority
ISP – Internet Service Providers
ITSU – IT Security Unit
MBA – Mauritius Bankers Association
MCCI – Mauritius Chambers of Commerce and Industry
MICCP - Ministry of Industry, Commerce and Consumer Protection
MICT – Ministry of Information & Communication Technology
MIH – Mauritius Institute of Health
MITIA – Mauritius IT Industry Association
MOBEC - Ministry of Business, Enterprise, and Cooperatives
MOE/HR – Ministry of Education and Human Resources
MOFARIIT – Ministry of Foreign Affairs, Regional Integration and International Trade
MOFED – Ministry of Finance and Economic Development
MOGECFW - Ministry of Gender Equality, Child Development and Family Welfare
MPA – Mauritius Ports Authority
MRA – Mauritius Revenue Authority
MSA– Mauritius Sugar Authority
MSB – Mauritius Standards Bureau
MTPA – Mauritius Tourism Promotion Authority
NCB – National Computer Board
NGO – Non-Governmental Organisations
OTAM – Outsourcing & Telecommunications Association of Mauritius
PMO – Prime Minister’s Office
SIL – State Informatics Limited
SLO – State Law Office
SMEDA - Small and Medium Enterprises Development Authority
TEC – Tertiary Education Commission

PART 1

Introduction

Vision, Mission And Goals For Cyber Security

1. INTRODUCTION

Societies are becoming increasingly more dependent on information and communication technologies which are globally interconnected. With these growing dependencies, information systems and networks are extremely vulnerable to disturbances which can affect their functioning. Cyber-security threats have become more sophisticated and have more serious repercussions than before. There is a growing misuse of electronic networks for criminal purposes or for objectives that can adversely affect the integrity of a nation's critical infrastructures. Cyber-attacks can be mounted at any time, against anyone and from anywhere. In a realm, where technology and change are speeding, responding effectively to cyber threats require a consistent and extensive effort. To address the cyber security issues in Mauritius, a National Cyber Security Strategy is required which will define the main goals, guidelines and action plans to respond effectively to cyber threats. The strategy also recognizes the fundamental challenge of balancing the measures intended to protect security.

By following the strategic guidelines and measures, Mauritius will be able to manage deliberate and unintentional disturbances in the cyber space as well as respond to and recover from them. The aspiration is that the action plans outlined in this strategy will position Mauritius where citizens know what to do to protect them; law enforcement is tackling cyber criminals; effective cyber security is seen as positive for business in Mauritius; online public services are secure and the threats to our national infrastructure and national security have been confronted.

The strategy provides an overview of what it takes to effectively protect information systems and networks and also gives an insight into the Government's approach and strategy for protection of cyberspace in the country. The cybersecurity strategic programmes which were set out in both NICTSP 2007-2011 and NICTSP 2011-2014 have been taken into account to build the cybersecurity strategic plan. The inputs have also been taken from the survey conducted on the State of Information Security in Businesses in Mauritius completed in October 2013. The purpose of the survey was to assess the security posture of businesses in Mauritius.

The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users including home users and small, medium and large enterprises and Government & non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to the security of cyberspace. It also enables individual sectors and organisations in designing appropriate cyber security policies to suit their needs.

2. VISION, MISSION AND GOALS FOR CYBER SECURITY

Vision

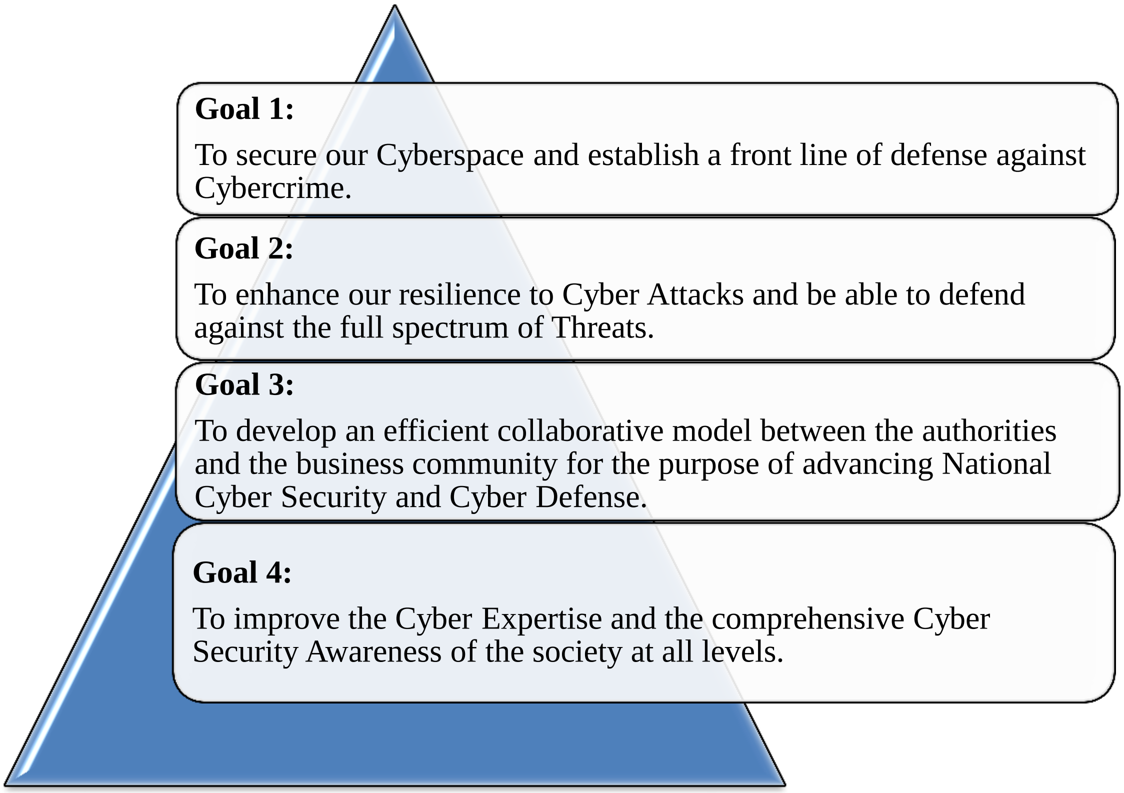
Our Vision is to enhance the cyber threat preparedness of Mauritius and managing the disturbances caused by these threats

Mission

Our Mission is to integrate Information Security firmly into the basic structures of our information society

Goals

To achieve this vision, we want:



Goal 1:

To secure our Cyberspace and establish a front line of defense against Cybercrime.

Goal 2:

To enhance our resilience to Cyber Attacks and be able to defend against the full spectrum of Threats.

Goal 3:

To develop an efficient collaborative model between the authorities and the business community for the purpose of advancing National Cyber Security and Cyber Defense.

Goal 4:

To improve the Cyber Expertise and the comprehensive Cyber Security Awareness of the society at all levels.

PART 2

Cyber Security Management And The Mauritian Approach

3. CYBER SECURITY MANAGEMENT AND THE MAURITIAN APPROACH

Preparing for cyber threats and cyber defense involve immediate, transparent and better coordinated action from all parties in society, both individually and collectively. It is important to provide political guidance and strategic guidelines for cyber security and take necessary decisions regarding the allocation of resources and prerequisites.

Cyber Security management requires that the different stakeholders have a reliable, real-time cyber security situation depiction of the condition of society's key functions and the disturbances which can affect their functions. The natures of threats highlight the importance of cooperation as well as efficient and flexible coordination.

National cyber resilience will be tailored to ensure the preparedness and predictive capabilities required by the goals and to facilitate its operating capability during cyber conflicts and post-conflict recovery.

3.1 Principles

<u>The Mauritian approach for managing cyber security is built on the following principles:</u>

1. Cyber security is a significant part of the comprehensive security of society. The approach for the implementation of the national cyber strategic plan is based on the set of goals for cyber security.

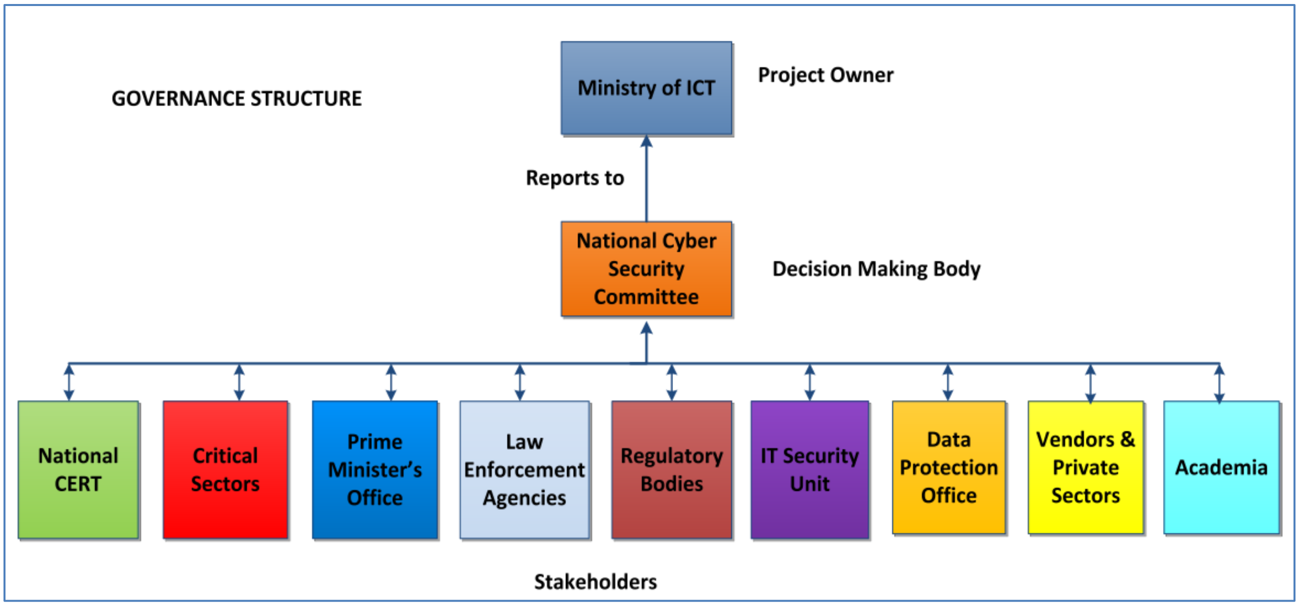
2. Cyber Security relies on the information security preparedness of the whole nation. The implementation of a CIIP framework will help in protecting the national critical information infrastructures. This will also include developing and offering expertise and advice, support and implement responses to threats or incidents and strengthen crisis management.

3. The methodology for the implementation of national cyber strategic action plan is established on efficient and comprehensive collection of information, an analysis and gathering system along with common and shared situation awareness, national and international cooperation in preparedness. This requires the establishment of an Anti-Cyber Threat Monitoring System which will aid to better respond, monitor and coordinate cyber threats at national level by operating on a 24/7 basis.

4. Cyber security is being constructed to meet its functional and technical requirements. A comprehensive framework will be set up to monitor Internet traffic which might be harmful to the nation and society.

5. In order to ensure cyber security development, Mauritius will see to it that appropriate legislations and incentives exist to support the business activities and their development in this field.

3.2 Proposed Governance Structure



To enable a collaborative working of all key players in public and private sector to safeguard the country's information infrastructure, a partnership of government, corporate and private stakeholders is important and will lead to the success of the implementation of the strategy. An effective public-private partnership for cyber security would provide the abilities to identify threats, anomalous behaviours, respond to them and will create a more secure network environment through better standardized security programs. This partnership will also set a stage to carry out research and development and find ways to mitigate security threats. Finally, this will also help to empower stakeholders to properly address cyber threats.

Stakeholders and their Roles

The different stakeholders and their roles towards this collaborative framework are described below:

Stakeholders	Roles
Ministry of ICT	• Acts as the Project owner and is responsible for setting-up of the necessary legal framework for strategy implementation.
National Cyber Security Committee	The National Cyber Security Committee acts as the decision making body and will include representatives from the MICT, National CERT (CERT-MU), Law Enforcement and Regulatory Bodies, Critical Sectors, PMO, Data Protection Office, Vendors & Private sectors and Academia to oversee and monitor the implementation of the strategy. The role of the National Cyber Security Committee will be to: • Lead activities associated with developing and managing national CIIP efforts, including coordinating policy development, outreach and awareness, risk assessment and management efforts, funding and support for the CIIP program efforts. • Serve as an important escalation functions for resolving important issues and emergencies.
National CERT	The National CERT (CERT-MU), a division of the National Computer Board is the advisory body for information security issues in the country. The responsibilities of the National CERT will be: • To implement the outputs generated from the cybersecurity committee. • To handle and coordinate cyber security incidents. • To monitor and analyse the information security situation at national level. • To prevent occurrence and recurrence of cyber incidents by developing incentives for cyber security compliance and proactive actions • To promote the adoption of best practices in information security and compliance.

	• To interact with government agencies, industry, the research community, and others to analyse cyber threats and vulnerabilities, disseminate reasoned and actionable cyber security information such as mitigations to the public.
Law Enforcement	Law Enforcement will be represented by members of the Police. Their roles will be to: • Enable effective prevention, investigation, and prosecution of various aspects of cybercrime that intend to steal information or compromise the integrity of critical operations.
Regulatory Bodies	The Regulatory bodies shall include the ICTA, IBA and the Bank of Mauritius (the financial sector regulator). The roles of the regulatory bodies will be to: • Establish, control, inspect and enforce regulations with regard to cyber security • Encourage organisations to adopt security best practices and guidelines
Critical Sectors	The critical sectors will include members from different the financial services (FSC, MRA), Tourism (MTPA), CEB, CWA, ICT & Broadcasting, Health (MIH), Government Services (GOC, CISD), Manufacturing (MEXA), Transport & Logistics (AML, MPA), Sugar (MSA) and Customs (MRA). The role of the critical sectors will be to facilitate identification, prioritization, assessment and protection of critical information infrastructure through information sharing and reporting.
Prime Minister’s Office (PMO)	The Representatives of the PMO would be the PMO Security Division and Counter Terrorism Unit. Their roles will be to advise and support the implementation of the strategy geared towards protecting Mauritius from cyber threats and attacks.
IT Security Unit	The IT Security Unit will establish IT Security best practices and promote implementation of information security standards within the Civil Service.
Data Protection Office	The Data Protection Office will act as the advisory body on data protection and privacy issues.

Academia	Academia will consist of members from the Tertiary Education Commission, the Universities and Tertiary Education Institutions. The roles of the academia will be to: • Encourage Research & Development to develop trustworthy and cost effective security solutions • Collaborate with industry in frontline technologies and solution oriented research • Develop educational and training programs for the formation of information security professionals and students
Vendors and Private Sectors	Vendors & Private Sectors will be represented through respective Associations. Their responsibilities will be to: • To advise on secure products and services which are critical to the information infrastructure operators and the general participants in the national economy • To provide strategic insights on security architecture, operations and risk management approaches to users • To provide patches and mitigation strategies in the face of attacks

PART 3

Strategic Guidelines For Cyber Security

Importance Of The National Cyber Security Strategy And Action Plan

4. STRATEGIC GUIDELINES FOR CYBER SECURITY

A national cyber security strategy is established in line with the strategic guidelines. This will create the conditions for the realization of the national cyber security vision. A separately prepared action plan will outline the measures to achieve the national cyber security goals. The implementation of the strategic guidelines will reinforce national and international cooperation. Such collaboration can best serve the whole society and support the stakeholders who play a significant role in the cyber security community. Cyber security is constructed on capabilities development over the long term, their convenience and flexible use and the resilience of society's key functions against the disturbances in cyber security.

Strategic Guidelines

	Guidelines
a	**To secure our Cyberspace and establish a front line of defense against Cybercrime** This initiative is aimed at building an approach to cyber defense strategy that prevents interference and attack in cyberspace by improving capabilities, articulating roles and developing appropriate responses for public and private sector. By creating or enhancing shared situational awareness of network vulnerabilities, threats and events and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions can help in securing our cyberspace. Additionally, this strategic guideline also emphasizes on enhancing the capacity of law enforcement agencies to investigate and prosecute cybercrime. Cyber defense against cybercrime will be exercised and developed together through international cooperation and the exchange of information.
b	**To enhance our resilience to Cyber Attacks and be able to defend against the full spectrum of threats** The strategic guidelines of the National Cyber Security Strategy are advanced by intensifying efforts to protect the critical infrastructure and networks in order to provide reasonable assurance of resilience and security to support national missions and economic stability. The well-being of the national economy, security and quality of life is becoming increasingly dependent on the safety and the robustness of critical infrastructures whose disruptions can affect a nation's ability to function effectively in crisis. Key importance is being given to government information infrastructure & systems which will be protected against cyber threats through security audits and implementation of national and international Information Security standards. The goal is to detect and identify any disturbances to the vital functions and to respond to them in a manner which minimizes their detrimental effects.

c	**To develop an efficient collaborative model between the authorities and the business community for the purpose of advancing National Cyber Security and Cyber Defense** The strategic guidelines of the Cyber Security Strategy are reinforced by strengthening active collaboration between actors whose aim is to achieve a shared situation awareness and effective defense against the cyber threats. A common set of criteria will be created to facilitate identification of critical IT infrastructures and systems. A method will be devised for risk and vulnerability assessments. Cyber defense will be advanced by promoting the exchange of information and regulations as well as through cooperation between the authorities and the business community.
d	**To improve the Cyber Expertise and the comprehensive Cyber Security Awareness of all societal actors** *Encouraging a cadre of cyber security professionals and building capacity to deter and defend against high-end threats* In a secure information society, everyone must be aware of the information security risks of their actions and their responsibility in preventing those risks. This strategy is intended to raise the level of competence by investing in the expertise of information security professionals and in the general awareness of information security of all actors. To continuously improve the competence and awareness of the actors, inputs will be made to promote the development of a cadre of skilled cyber security professionals and capacity building so that Mauritius can retain an edge in this area and development to keep producing innovative solutions operations in cyberspace. By promoting awareness of the need for cyber security, the Strategy will encourage individuals, Industry and all levels of government to adapt behaviour and adopt the technology required to confront evolving cyber threats. The cooperation between industry and academia on knowledge sharing in information security areas will also be promoted by holding regular annual conferences on information security targeting major players and participants in the region.

5. IMPORTANCE OF THE NATIONAL CYBER SECURITY STRATEGY AND ACTION PLAN

The ICT sector is influencing the lives of people through direct or indirect contribution to the various socio-economic parameters such as employment and standard of living. It is playing a significant role in transforming Mauritius into a cyber-hub in the African region. The Government has also been a key driver for increased adoption and promotion of IT based products and IT enabled services in the public services (e-Government services to citizens), education (e-learning, virtual classrooms) and financial services (mobile banking, Internet banking). Such initiatives have enabled increased IT adoption in the country.

In the light of the growth of the ICT sector in Mauritius, providing the right focus for creating a secure computing environment has become one of the compelling priorities for the country. Cyber space is vulnerable to a wide variety of incidents which could hamper economic, public health, safety and national security activities. Reputation, trust and brand value can all be seriously affected by information loss and theft.

However, with rapid identification, information exchange, investigation and coordinated response and remediation, the damaged caused by malicious activities can be mitigated. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information is the essence of a secure cyberspace.

Due to the dynamic nature of the cyberspace, there is a need to address the security challenges and issues. These actions are unified under a **National Cyber Security Strategy** which sets out guidelines, measures and action plans that will provide reasonable assurance of resilience and security to support national missions and economic stability. A secure society makes it easier for both individuals and businesses to plan their activities, which in turn boosts economic activity as well as improve the country's appeal for international investors. The implementation of the strategy is planned over a period of 5 years from 2014 to 2019.

PART 4

National Cyber Security Strategic Action Plan

6. NATIONAL CYBER SECURITY STRATEGIC ACTION PLAN 2014 - 2019

GOAL 1: TO SECURE OUR CYBERSPACE AND ESTABLISH A FRONT LINE OF DEFENSE AGAINST CYBER CRIME

Approach	Project Code	Project Name	Description	Lead	Stakeholder(s)	Priority	Start Date	End Date
Tackling cyber security • Reducing online vulnerability • Limiting criminal activity online • Stimulating more effective partnerships **Making it safer to do business in cyberspace** • Increasing awareness and visibility of threats • Improving Incident Response • Protecting Information and Services • Fostering a culture that manages the risks • Promoting confidence in cyberspace	CS1P1[1]	Setting up of a Cyber Threat Monitoring System	To better respond, monitor and coordinate cyber threats at national level. It will also include a cyber-forensics lab for carrying out forensic activities.	**CERT-MU**	MICT ICTA ITSU DPO POLICE PMO ISPs	High	2014	2016
	CS1P2	Setting up of a content filtering system to block illicit materials on ICT devices	For controlling and blocking access to age-sensitive content on mobile devices.	**MICT**	MICT CERT-MU ICTA ISPs DPO POLICE ITSU	High	2015	2016
	CS1P3	Establish a mechanism for the removal of illegal contents	This mechanism will help to remove online illegal child content after it has been identified.	**CERT-MU**	MICT ICTA POLICE MOGECFW NGO's	High	2015	2016
	CS1P4	Conducting Cyber Security Drills	To conduct regular cyber security drills and exercises at national and organizational level to evaluate the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.	**CERT-MU** **ITSU**	MICT ICTA POLICE CRITICAL SECTORS	High	2015	2017
	CS1P5	Enhance Law Enforcement capability on cybersecurity	• To develop new training, giving more capability to understand and investigate cybersecurity.	**POLICE**	MICT SLO CERT-MU ICTA	High	2015	2019

[1] CS1P1 – Cyber Security Strategic Goal 1 Project 1

			• To incorporate electronic evidence and introductory cybercrime training within the curriculum for law enforcement agencies. • To include training on cybercrime and electronic evidence for all new police recruits.		DPO			
	CS1P6	International and Regional Cooperation on cybercrime	To promote greater levels of cooperation regionally and internationally and shared understanding on cyber-crime.	**CERT-MU**	MICT ICTA ITSU DPO POLICE MOFARIIT	High	Ongoing	
	CS1P7	Enhance the security of cyberspace	To develop effective public private partnership and collaborative engagement through technical and operational cooperation between authorities and business community.	**CERT-MU**	MICT ICTA ITSU DPO POLICE PMO ISPs CRITICAL SECTORS	High	2014	2019
	CS1P8	Legal Framework Assessment	• To develop a dynamic legal framework and its periodic review to address cyber security challenges arising out of technological developments in cyber space and its harmonization with international frameworks. • To introduce in the law the possibility to intercept communications on real-	**MICT**	CERT-MU SLO ICTA ITSU DPO POLICE ISPs	High	2014	2016

			time and to retain traffic data for a specific period of time.					
GOAL 2: TO ENHANCE OUR RESILIENCE TO CYBER ATTACKS AND BE ABLE TO DEFEND AGAINST THE FULL SPECTRUM OF THREATS								
Approach	**Project Code**	**Project Name**	**Description**	**Lead**	**Stakeholder(s)**	**Priority**	**Start Date**	**End Date**
Defending our national infrastructure from cyber attacks • Reinforcing defenses in cyber space • Improving resilience and reducing the impact of cyber attacks **Ensuring that Mauritius has the capability to protect our interests in cyber space** • Improving our ability to detect threats in cyber space • Increasing our capability to prevent and disrupt attacks on Mauritius	CS2P1	Develop and Implement a CIIP Framework	To protect the national critical information infrastructures and setting up of sectoral CERTs to coordinate and communicate actions within respective sectors for effective incident response and resolution and cyber crisis management.	**CERT-MU**	MICT ICTA ISPs CRITICAL SECTORS DPO MITIA POLICE ITSU PRIVATE SECTORS	High	2014	2015
	CS2P2	Development and Implementation of a Cyber Crisis Management Plan	To enable organisations to respond to cyber incidents and assess the preparedness of organisations to withstand cyber-attacks.	**CERT-MU**	ITSU ICTA DPO PMO ISPs CRITICAL SECTOR POLICE	High	2015	2018
	CS2P3	Provision for Fiscal Schemes and Incentives	To encourage organisations to install, reinforce and upgrade information infrastructure with regard to cyber security.	**CERT-MU**	MICT MOFED SMEDA MOBEC	Medium	2016	2017
	CS2P4	Creation of a national test-bed for network security	To provide a secure and resilient infrastructure by encouraging all organizations to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and networks.	**MICT** **MOFED**	CERT-MU ITSU ISPs VENDORS ACADEMIA CRITICAL SECTORS CISD	Medium	2016	2019

	CS2P5	Adoption of a Cyber Security Controls Scheme for protection against cyber threats	To mandate the implementation and accreditation of a Cyber Security Controls Scheme within organisations. This will provide the basic but essential level of protection within organizations' IT systems in order to mitigate the risks emanating from cyber threats.	**CERT-MU**	MICT ITSU MOFED SMEDA MOBEC MSB	High	2015	2019

GOAL 3: DEVELOP AN EFFICIENT COLLABORATIVE MODEL BETWEEN THE AUTHORITIES AND THE BUSINESS COMMUNITY FOR THE PURPOSE OF ADVANCING CYBER SECURITY

Approach	Project Code	Project Name	Description	Lead	Stakeholder(s)	Priority	Start Date	End Date
Helping to shape the development of cyber space • Promoting an open and interoperable cyberspace • Protecting our way of life • Ensuring security without compromising our values	CS3P1	Promote Information Risk Management at National level	To promote Information Risk Management using standard frameworks such as NIST's Framework for Cybersecurity within public and private sector.	**CERT-MU**	ITSU RISK MGT FIRMS	High	Ongoing	
	CS3P2	Promote the universal adoption of Information Security standards at National level	To adopt the implementation of security standards such as ISO 27001, ISO 27003, ISO 27004, ISO 27005, ISO 27006.	**CERT-MU**	MSB ITSU SGS	Medium	Ongoing	
	CS3P3	Promote Secure software Development	To encourage secure software development processes based on global best practices.	**CERT-MU**	MICT ACADEMIA MITIA	High	2015	2018
	CS3P4	Promote the designation of a Senior Information Security Personnel (CISO, IS Consultants, Information Security Experts) within organisations	To encourage all organisations, private and public to designate member of a senior management as Chief Information Security Officer, IS Consultants, Information Security Experts responsible for security efforts and initiatives.	**CERT-MU**	APPLICABLE TO ALL SECTORS	Medium	2017	2019
	CS3P5	Promote the implementation of Information Security Standards in the Civil Service	ISMS to be implemented for Ministries and Departments with Critical Information Systems	**ITSU & Line Ministries**	MICT CIB CISD	High	2014	2019

	CS3P6	To promote e-Government initiatives and ensure conformance to security best practices.	To mandate the implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Government initiatives to decrease the risk of disruption and improve the security posture.	**Line Ministries/ Department**	MICT CERT-MU ITSU GOC CIB CISD	High	2014	2019
	CS3P7	Adoption of guidelines for procurement of ICT products	To encourage organisations to adopt guidelines to procure trustworthy ICT products and provide the procurement of manufactured ICT products that have security implications.	**ICTA**	MICT CERT-MU ITSU CIB CISD PUBLIC PROCUREMENT OFFICE MRA Ministry of Industry, Commerce & Consumer Protection	Medium	2017	2019
	CS3P8	Conducting mandatory Information Security Audit	To make security audit mandatory on a periodic basis for assessing the organisation's security posture, including critical information infrastructure.	**MICT**	CERT-MU ITSU SLO ICTA CIB MOFED DPO BANK OF MAURITIUS	High	2014	2016
	CS3P9	Collaboration with industry for research and development	• To collaborate jointly with industry and academia to support the application of research for building innovative cyber security solutions and enhance our technical capabilities to support our national security interests and	**CERT-MU**	MICT ITSU ACADEMIA MRC Industry Associations	Medium	2017	2019

			wider economic prosperity. • To enlarge and strengthen the cyber security research community by formalising the coordination and prioritisation of cyber security research and development activities.					
	CS3P10	To establish a collaborative framework with vendors and service providers to improve the visibility of the integrity of ICT products and testing and validating the security of such products.	• To foster trusted relationships with product/system vendors and service providers for improving end-to-end supply chain security visibility. • To encourage a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.	**ICTA**	MICT ITSU CERT-MU Industry Associations MICCP PROCUREMENT OFFICE MINISTRY OF INDUSTRY & COMMERCE	Medium	2017	2019

GOAL 4: TO IMPROVE THE CYBER EXPERTISE AND THE COMPREHENSIVE CYBER SECURITY EDUCATION & AWARENESS OF ALL SOCIETAL ACTORS

Approach	Project Code	Project Name	Actions to Include	Lead	Stakeholder(s)	Priority	Start Date	End Date
Extending knowledge • Building a coherent cross-sector agenda • Deepening understanding of the threats, vulnerabilities and risks **Enhancing skills** • Building a culture that makes people	CS4P1	Promote security certifications and trainings from renowned International organisations	To promote security certifications from organisations such as EC-Council, OWASP, ISC2, SANS amongst others can be considered for security professionals.	**CERT-MU**	MICT ITSU ICTA ACADEMIA INDUSTRY ASSOCIATIONS	Medium	2016	2019
	CS4P2	Establish cyber security training programmes for SMEs	To establish cyber security training programmes for SMEs. This will help to foster a culture of information security within the SME sector.	**NCB (CERT-MU)** **SMEDA**	MICT MINISTRY OF BUSINESS ENTERPRISE INDUSTRY	Medium	2016	2019

understand risks and enable them to use cyberspace securely.					ASSOCIATION ICTA			
Expanding capability • Building technical capabilities • Increasing ability to respond to incidents	CS4P3	Cyber Security Education	To improve educational involvement with cyber security at all levels (primary, secondary and tertiary) through curriculum development and research.	**TEC** **MOE/HR**	MICT CERT-MU ICTA ITSU POLICE DEPT	High	2014	2019
	CS4P4	Cyber Security Awareness in Civil Service	To improve Cyber Security Awareness and Education in Civil Service	**ITSU**	MICT MCSAR	High	2014	2019
	CS4P5	Organisation of International Cyber Security annual events	To hold regular annual conferences on information security targeting major players and participants in the region.	**MICT**	CERT-MU ICTA	Medium	2015	2019