Republic of Mauritius

NATIONAL CYBERSECURITY STRATEGY 2023-2026

For a **more secure** and **resilient Mauritius**

Computer Emergency Response Team of Mauritius

NATIONAL CYBERSECURITY STRATEGY 2023-2026

For a more secure and resilient Mauritius

TABLE OF CONTENTS

NATIONAL
CYBERSECURITY
STRATEGY 2023-2026
For a more secure and resilient Mauritius

MINISTER'S FOREWORD

Minister's Foreword

Honourable Deepak Balgobin
Minister of Information Technology, Communication and Innovation

As the world becomes increasingly interconnected, cyberthreats continue to grow and evolve exponentially. Moreover, with the rapid adoption of advanced technologies such as machine learning, artificial intelligence, and a reliance on data analytics, there are now more points of vulnerability for cyber attackers to exploit and launch sophisticated attacks. Mauritius is also no safe haven from these threats. Statistics gathered from the Mauritian Cybercrime Online Reporting System (MAUCORS) clearly support this fact. Therefore, our response to address these cyber threats must be bold and long lasting.

Therefore, the new National Cybersecurity Strategy 2023-2026 has been developed, which is our plan to ensure that Mauritius remains capable and resilient in this fast-moving digital world. Through this Strategy, the Government's aim is to strengthen the security and resilience of critical information infrastructure against cyber threats, ensure that our legal framework remains strong and resilient to cybercrime, promote collective responsibility for cybersecurity, promote innovation, enterprise security and cybersecurity education and finally strengthen regional and international partnership.

Our work to make Mauritius cyber secure does not end here. Preparing for cyber threats and defense involve immediate, transparent and better coordinated action from all parties in society, both individually and collectively. The Government will continue to work hand-in-hand with relevant stakeholders to promote cybersecurity, provide political guidance and take the necessary decisions regarding the implementation of projects to achieve cyber resilience. A Monitoring and Evaluation exercise will also be undertaken regularly to measure the progress of the Strategy implementation.

This Strategy has been developed with the assistance of several stakeholders who participated in the consultation exercise. I would also like to thank them as well as regional and international partners who have reviewed the strategy and provided us with their valuable feedback. Lastly, I would also like to thank my Ministry for their commitment and advice which has been fundamental towards the development of this Strategy.

NATIONAL
CYBERSECURITY
STRATEGY 2023-2026

For a **more secure** and **resilient Mauritius**

INTRODUCTION

Introduction

Information and communication technologies have evolved over time and has now integrated into virtually every aspect of our lives. Mauritius is now a digitalised society. The transformation brought by this digitalisation creates new dependencies. Our economy, the Government and critical sectors now rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. A loss of trust in that integrity would jeopardize the benefits of this technological revolution.

The Mauritian response to the COVID-19 pandemic has shown the importance of secure online connectivity. Mauritians are rightfully seizing the opportunities of the digital world to interact and work online, trusting the internet for healthcare, working from home, education, entertainment, online shopping, amongst others. However, as more people are moving online, new cyber threats are also rising. Cyber-attacks are becoming more sophisticated and cyber criminals are doing great harm by infiltrating systems from anywhere in the world, stealing money, identities and data. They are taking advantage of COVID-19 to target government, communities and businesses. Through the dark web, numerous illicit cyber activities are being carried out including sharing abhorrent images of child abuse. It is more important than ever to protect our citizens online from those who would do us harm.

The 2014-2019 National Cybersecurity Strategy had set out the Government's commitment to address cyber threats and measures were undertaken to strengthen Mauritius cyber resilience. The policies, institutions and initiatives developed over the last five years is helping to establish Mauritius as a leading regional player in cyber security and build our global influence. Nevertheless, with emerging technologies and evolution of new threats, there is a need to constantly improve our cyber defenses and national response against these threats. The new cybersecurity strategy is built on the existing foundation and puts forward new initiatives to further strengthen the Mauritian cyberspace. The strategy represents an ambitious, interventionist approach to defend our people, country and develop our capabilities. The successful implementation of this strategy will make our citizens and businesses more secure and and underpin our future prosperity as a digital economy as well as help Mauritius on the regional and international fronts.

NATIONAL CYBERSECURITY STRATEGY 2023-2026

For a more secure and resilient Mauritius

SCOPE OF THE STRATEGY

Scope of the Strategy

The 2014 -2019 National Cybersecurity Strategy has brought significant developments and the Mauritian cyberspace is more resilient against cyber threats. As per International Telecommunication Union (ITU) Global Cybersecurity Index, Mauritius is the top ranked in the African region since 2014. Undeniably, this ranking reaffirms the position of Mauritius as destination which provides a robust and secure ICT ecosystem in the region.

This strategy reaffirms the intention to shape the Government's policy, while also offering a coherent and compelling vision to share with the public and private sector, academia and the wider population. The strategy sets out proposed or recommended actions aimed at all sectors of the economy and society, from ministries and departments, to leaders across the industry and the individual citizen.

Relying on the challenges that we faced and building on achievements of the 2014 strategy, this document sets out:

- An assessment of the cyber threat landscape, including current and evolving threats.
- A review of vulnerabilities and how they have developed over the last 5 years.
- The Government's vision for cybersecurity for the period of 2023-2026 and the key objectives to achieve the goals.
- How to put the policy into practice and the intention to assess the progress towards our objectives.

Strong Foundation – Our Key Achievements

In the five years since its inception, the National Cyber Security Strategy 2014-2019 has provided a road map for Mauritius to fight against cyber threats and strengthen our resilience. It has helped to establish Mauritius as a regional leader in cybersecurity as other countries considering our strategy as a model for a comprehensive, forward looking approach. This Strategy brought together partners across governments, private sectors and the wider society to protect our cyberspace and develop our capabilities. It has also helped to tackle cybercrime, increase the cybersecurity resilience of businesses and educate our citizens on cyber threats. The key achievements of this strategy are as follows:

- Setting up of the Mauritius Cyber Threat Information Sharing System (MAUSHIELD)
- Declaration of Mauritius as a Cybersecurity Hub for the African region by the Cyber4Dev
- Cybersecurity and Cybercrime Act 2021 proclaimed and enforced in December 2021
- The operationalization of the Mauritian Cybercrime Online Reporting System (MAUCORS)
- The finalization of the National Cyber Incident Response Plan
- Establishment of the Critical Information Infrastructure Protection Framework in the Cybersecurity and Cybercrime Act 2021
- Organization of national and international cyber drills
- Setting up of the topnotch committee known as the National Cybersecurity Committee
- Establishment of Child Online Safety programmes
- Promotion of Cybersecurity-as-a-service
- Promotion of international cybersecurity standards and best practices
- Operationalisation of the ITU Centre of Excellence (CoE) in the field of Cybersecurity
- Creation of national and regional cybersecurity talent pipeline through the ITU CoE
- Operationalization of the Security Operations Centre for the Government
- Enhancement of regional and International cooperation in the new Cybersecurity and Cybercrime Act 2021.
- Promotion of information cybersecurity culture through different target audience including physically challenged children
- Promotion of national, regional and international platform for information exchange through hosting fora's and symposiums.

NATIONAL
CYBERSECURITY
STRATEGY 2023-2026

For a more secure and resilient Mauritius

CYBER THREATS AND CHALLENGES

Cyber Threats and Challenges

Cyber security is at the heart of the transition of a digital society. It is a key pillar in ensuring a trusted and secure digital economy, giving confidence to all participants and allowing businesses to prosper and thrive. The rapid and widespread uptake of digital technology by households and businesses following the COVID-19 pandemic underscores the importance of digital technology as an economic enabler. Hundreds of Mauritians are working from home, staying connected through apps and using essential services. Many bricks and mortar businesses are moving online.

However, with the COVID-19 pandemic, the nature of cyber threats has evolved considerably. Opportunist cyber criminals quickly adapted their methods to take advantage of the situation as more people are working, studying and connecting online. Affordable and low-tech attacks such as online scams, ransomware, phishing and malware will continue to rise. The stability and prosperity of any country largely depend on the security and reliability of cyberspace which can be jeopardized by technical causes, social media based threats, natural phenomena or deliberate aggressions.

a) Social Media based threats

Social media has become a popular platform in Mauritius for communicating, sharing life experiences, pictures, videos and even buying and selling stuffs. The most popular examples of social media platforms used in the country are Facebook, Instagram, WhatsApp and TikTok. Professionals prefer LinkedIn for job postings and developing networks. The number of Mauritians using social media has increased drastically.

However, the number of incidents related to social media rose exponentially. Incidents related to social media such as online harassment, cyber bullying, sextortion, identity theft, compromised accounts, online scams have also increased. With the COVID-19 pandemic, as well as evolvement of technologies and new techniques being used by malicious people, cyber threats related to social media has proliferated. As the social media is being used as the platform to communicate and shop during lockdowns, cybercriminals have leveraged by conducting illicit activities. A significant increase was noted in the number of social media based threats reported on MAUCORS during the lockdown period.

Cyber Threats and Challenges (continued)

b) Malicious attacks

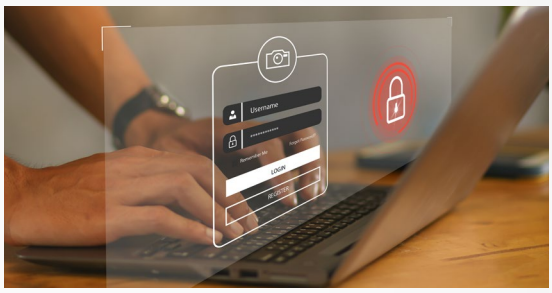
Malicious attacks such as ransomware continue to create havoc. While ransomware is not a new threat, threat actors are growing bolder and more sophisticated as their methodologies are evolving. One of the main trends is the employment of additional extortion tactics such as leaking stolen information, publishing the incident to the media, notifying the victim's partners and customers of the incident, amongst others. Another trend is the rise of the Ransomware-as-a-Service (RaaS) business model that allows ransomware developers to lease their tools and techniques to other criminals, thus, giving them access to sophisticated tools and methods. The damage caused have pushed governments to seek solutions. Many of the solutions pursued focused on coordinating government-wide efforts and law enforcement operations aimed at disrupting and deterring cybercriminal groups operating from foreign countries as well as rendering the ransomware market unprofitable by seizing the ransom paid. Mauritius is not the exception and has faced similar challenges.

c) Natural Disasters or Phenomena

When it comes to natural disasters, the first thing that comes to mind is saving lives. Cybersecurity rarely comes to mind in these instances, and hackers are well aware of this. Therefore, it is a must to understand how cybersecurity and natural disasters can affect you and your business. In the past, there have been several occurrences of cybercriminals taking advantage of a natural disaster by launching attacks such as phishing, online scams and social engineering, with the aim to steal personal and sensitive data.

Mauritius also has witnessed a rise in the number of phishing scams during the COVID-19 pandemic. Email is the main method used by cybercriminals to make their way into networks. The social engineering tactics they use to get people to click bad links or download bad attachments are even easier in the wake of a physical disaster. Often, they will impersonate charities raising money for victims or disaster relief agencies giving instructions, but any links or attachments will really download malware to the victim's computer. Other scams would also involve hackers standing up fake websites that purport to have data or updates about the event or disaster. They share the links to these websites via social media, preying on people who are desperate for information.

Cyber Threats and Challenges (continued)



d) Unpatched Security Vulnerabilities

While there are, countless new threats being developed daily, many of them rely on old security vulnerabilities to work. Since many businesses fail to patch vulnerabilities once they are identified, cybercriminals take the advantage by exploiting the same vulnerabilities. It is too common for a business or even just the individual users on a network to dismiss the "update available" reminders that pop up in certain programs because they do not want to lose the 5-10 minutes of productive time that running the update would take. Updating is a nuisance to most users. However, it is a "nuisance" that could save a business untold amounts of time, money, and lost business later. The country has faced this situation where organisations were targeted because of this particular flaw.

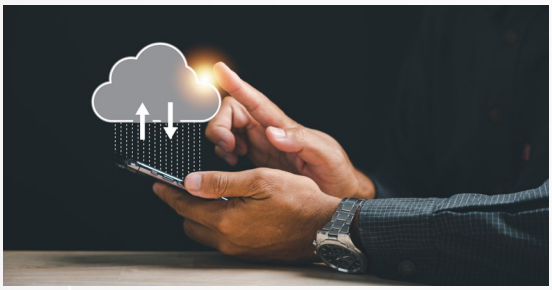
e) Superuser or Admin Account Privileges

One of the most basic tenets of managing software vulnerabilities is to limit the access privileges of software users. The less information/resources a user can access, the less damage that user account can do if compromised. However, it has been observed that many organisations fail to control user account access privileges, allowing virtually every user in the network to have so-called "Superuser" or administrator-level access. Some computer security configurations are flawed enough to allow unprivileged users to create admin-level user accounts. Verifying that user account access is restricted to only what each user needs to do their job is crucial for managing computer security vulnerabilities. Also, ensuring that newly-created accounts cannot have admin-level access is important for preventing less-privileged users from simply creating more privileged accounts.

Cyber Threats and Challenges (continued)

f) Employees and Insider Threats

One of the biggest security vulnerability in any organization is its own employees. Whether it is the result of intentional malfeasance or an accident, most data breaches can be traced back with the implementation of appropriate technological or security solution. It has been reported that employees have abused their access privileges for personal gain, others have also clicked on links in emails and downloaded malicious files or have even deliberately or unintentionally submitted user account credentials to scammers or cybercriminals.



g) Cloud breaches

More and more companies are migrating to the cloud for remote working and to assure business continuity. Cybercriminals are following the same trend and targeting the cloud more frequently. Cloud-based security risks, including cloud misconfigurations, incomplete data deletion, and vulnerable cloud-apps, are noted as the most common sources of cyberattacks.

h) Internet of Things (IoT) attacks

Global organisations are increasingly deploying Internet of Things (IoT) devices and applications to accelerate operations, capture more data, manage infrastructure remotely, improve customer service, especially in industries such as manufacturing, retail, health, amongst others. In addition, we can find that individuals also are adopting IoT by making use of smart devices. However, the data-driven characteristics of IoT technologies expose the individual to privacy risks. Therefore, the possibility of collecting and processing sensitive information without human intervention is also a huge security threat. Cybercriminals can exploit IoT vulnerabilities to gain control of devices for use in botnets and to penetrate your network. What makes IoT technology so convenient is also what makes it so vulnerable: enhanced connectivity and convenience come with more security risks. This kind of threat is on the rise in the country.

Our society's degree of reliance on digital technology and cyberspace is growing exponentially with time. Knowledge of threats, managing the risks and building an appropriate prevention, defense, detection, analysis, investigation, recovery and response capability are essential elements of this National Cybersecurity Strategy.

NATIONAL CYBERSECURITY STRATEGY 2023-2026

For a **more secure** and **resilient Mauritius**

CONSULTATION

Consultation

For the review of the national strategy, the Ministry of Information Technology, Communication and Innovation has formed different working groups, comprising of representatives from different sectors namely public, private, critical, academia, regulatory bodies, law enforcement and judiciary. The approach followed, first of all was to carry out the gap assessment based on the existing cybersecurity threat landscape.

The questions addressed were as follows:

- What is the current status?
- The need for a new strategy
- Positioning ourselves in the future: The approach
- Focus areas and
- The way forward

Following the assessment, the groups have focused their discussion around the following thematic areas:

- Evolution of the cyber threat landscape
- Cyber threats targeting Mauritius and the growth of cybercrime
- Emerging technologies and associated threats
- Public and private partnership
- Information sharing and National Incident Response
- Cybersecurity Education and forming cybersecurity professionals
- Law enforcement capability to tackle cybercrime
- Legislations and regulations
- Procedures for combatting cybercrime
- SMEs and cybersecurity
- Economic opportunities for Mauritius
- Research and Development
- Positioning Mauritius in the future

The groups have come up with different views and recommendations to formulate the new strategy. The Ministry of Information Technology, Communication and Innovation has conducted a consultation workshop along with all relevant stakeholders to finalize the strategy document.

NATIONAL
CYBERSECURITY
STRATEGY 2023-2026

For a **more secure** and **resilient Mauritius**

OUR STRATEGY

Our Strategy

To address cyber threats and safeguarding our interests in cyberspace, we need a strategic approach that underpins all our collective and individual actions in the digital domain over the next three years. This section sets out our vision and strategic approach. It also helps to establish general guidelines for the secure use of cyberspace, encourage a comprehensive vision, the application of which will help to achieve maximum security and progress through the coordination and cooperation of stakeholders in the public and private sectors. The strategy also encourages Mauritius presence in regional and international front to protect cyberspace.

Our Vision

Our Vision is to make Mauritian cyberspace more secure and resilient against cyber threats.

The Guiding Principles

The National Cybersecurity Strategy is upheld and inspired by the governing principles of National Security and these are as follows:

NATIONAL
CYBERSECURITY
STRATEGY 2023-2026

For a **more secure** and **resilient Mauritius**

THE PILLARS

Pillar 1 – A Resilient Infrastructure

Cyber-attacks are increasingly frequent, sophisticated and impactful. There is a rise in the number of cyber threats such as ransomware, online financial fraud, cyber espionage and disruptions to Internet services. Attacks on systems that run utility plants, transportation networks, hospitals and other essential services are more recurrent. Successful attacks result in disruptions which could cripple economies. Left unchecked, malicious entities can find more ways to launch attacks, steal data and make cyberspace dangerous for all.

The protection of critical information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space. It is important to have a resilient infrastructure and trusted cyber environment which provides cost-effective business, service continuity, sustained revenue and uninterrupted delivery of critical services. To that end, measures should be taken to protect our critical infrastructures, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

With a view to enhancing the resiliency of critical infrastructure in Mauritius, the strategic objectives for a resilient infrastructure are as follows:

Objective 1: Strengthen the security and resilience of critical information infrastructure against cyber-attacks and other hazards

Supporting the continuity of critical services in the face of disruptive or sophisticated attacks is a fundamental obligation for the Government. The disruption of these services could have a disturbing impact across the country. It is therefore important to take the necessary measures to strengthen the security and resilience of the country's critical infrastructure against cyber threats.

In this perspective, provisions have been made in the new Cybersecurity and Cybercrime Act 2021 to protect the critical infrastructure of Mauritius.

Under this act, critical infrastructure should take the following measures:

- Conduct an assessment of the threats, vulnerabilities, risks and probability of a cyber-attack of the critical information infrastructure based on international best practices.
- Measure the overall preparedness against damage or unauthorised access to a critical information infrastructure;
- Identify any other risk based factors appropriate and necessary to protect the critical information infrastructure and integrate into the information security policy;
- Conduct periodic IT Security Risk Assessment of a critical information infrastructure; and
- Implement an incident reporting policy.

Pillar 1 – A Resilient Infrastructure (continued)

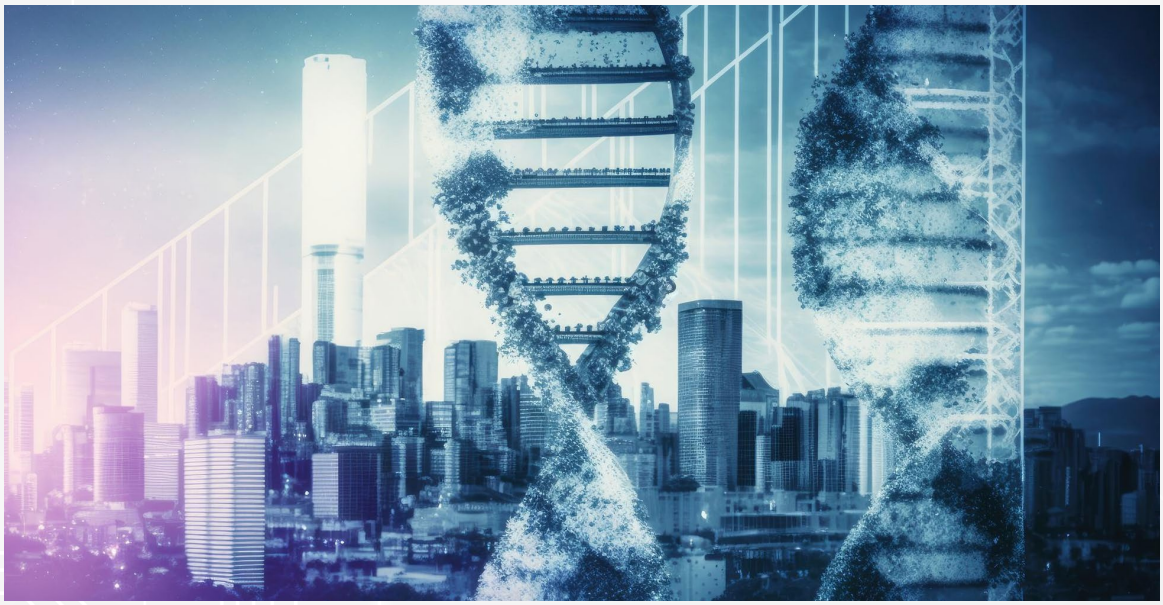
Objective 2: A dynamic and harmonized legal framework to effectively address the cyber security challenges

In order to ensure that Mauritius legal framework remains strong and resilient to cybercrime, it is important that it is aligned with the technological developments, international norms and standards, as well as legal and regulatory changes. In this perspective, a new Cybersecurity and Cybercrime Act has been developed and proclaimed in December 2021.This Act is also aligned with the Budapest Convention on Cybercrime as well as with the African Union Convention on Cybersecurity and Personal Data Protection to coordinate and manage trans-border issues. The new Cybersecurity and Cybercrime Act 2021 sets parameters which will enhance the security of the Mauritian cyberspace and boost its image as a trusted cyber territory in the region as well as globally.

In addition, to govern the protection of personal data in Mauritius, the Data Protection Act 2017 plays an important role. It is aligned with the EU's General Data Protection Regulation (GDPR) and Mauritius has also ratified the Convention 108+ in September 2020 to protect the right to privacy of individuals.

To achieve the objectives, the following measure will be undertaken:

- Enhance the development of incident response and recovery capabilities of critical sectors;
- Promote IT security risks assessment on critical infrastructures, including data protection impact assessments;
- Promote self-regulation among data controllers and data processors;
- Enhancing the scope of Government Security Operations Centre's (SOC) to a national SOC;
- Provision of benefits for adoption of standard security practices, processes and regulations; and
- Promote the adoption of international cyber norms and capacity building measures.



Pillar 2 – A Safer Cyberspace

Digital connectivity has both empowered and jeopardized businesses and individuals. It opens new social and commercial opportunities, yet also exposes citizens to criminal syndicates across the world. By commandeering computing devices, these malicious actors can steal data, extort money, and attack networks, causing harm to others. Cyberspace needs to be kept safe and trustworthy for businesses and individuals to benefit from it.

The strategic objectives for a safer cyberspace are:

Objective 1: Tackle Cybercrime and Improve Incident Reporting

Criminals from anywhere across the globe can use the internet to harm citizens with ease and at scale. To hold cyber criminals to account and prevent cybercrime, law enforcement agencies will need to collaborate with other partners to prevent or respond to malicious cyber activities, including in response to sophisticated cyber threats. This strategy will encourage law enforcement to enhance their technical cyber capabilities and cooperate with regional and international partners in the investigation and prosecution of cybercrime.

It is important to have a threat sharing platform that will enable critical infrastructure operators to share cyber threat intelligence about malicious cyber activities. To reduce the impact of cyber threats, their features should be known to best tackle them. Incident reporting contributes to identifying trends, fostering cooperation and information sharing. Besides their diversity, reporting makes a positive contribution to the fight against cybercrime. The prompt reporting of cyber incidents is essential to an effective response, linking of related incidents, identification of the perpetrators, and prevention of future incidents.

Pillar 2 – A Safer Cyberspace (continued)

Objective 2: Promote Collective Responsibility for Cybersecurity

Cybersecurity is the collective responsibility of everyone - the Government, business and the society. It is a way of putting total defence into action to keep Mauritian citizens safe. Everyone has a role in to play in the creation of a safer cyberspace.

Government

The Government will take measures to strengthen the country's cyberspace, businesses and critical infrastructure from cyber threats

Business

Businesses should take responsibility for securing their products and services and protect their customers from known vulnerabilities

Society

The society should take responsibility for practising secure online behaviours

To achieve these objectives, the following actions will be undertaken:

- Increase the capacity and capability of law enforcement agencies in the identification, investigation and prosecution of cybercrime;
- Ensure that legal professionals have access to information and resources that provide them with the necessary level of knowledge in the judicial field to apply the associated legal and technical framework more effectively;
- Enhance the capacity of CERT-MU to deliver new services;
- Encourage businesses and citizens to report incidents;
- Promote regular information security health checks of critical information infrastructures; and
- Establish a hybrid forum for facilitating discussions on cybersecurity issues.

Pillar 3 – Promote Innovation, Enterprise Security and Cybersecurity Education

Future economic growth in Mauritius will be boosted by access to new markets and the development of new forms of wealth creation. Disruptive technologies will open up new business opportunities, but many of these depend on trust and confidence in the security of cyberspace. Getting cyber security right will mean Mauritius is a secure and dynamic location for business diversification and investment.

The strategic objectives to promote innovation, enterprise security and cybersecurity education are:

Objective 1: Make Mauritius a Secure destination in the World to do business

This strategy will focus on measures that will have a combined effect of making the internet more secure for all our citizens. By ensuring the Government has the capacity and capability to counter cyber threats and confront illegal behaviour, businesses and the community will be exposed to fewer risks. Equipping small business owners and the community with the information and tools they require to protect themselves will encourage greater adoption of cyber secure products and cyber smart decision-making and hence making Mauritius as one of the most secure places in the world to do business in cyberspace.

Objective 2: Improve Mauritians Cyber Security Knowledge, Skills and Capabilities

Skilled and well-trained professionals are required to assess, design, develop and implement cybersecurity solutions and strategies. While the demand for cybersecurity professionals is high, the supply is low. To build on tomorrow's workforce, this strategy focuses on improving cyber security education at all levels of the education system. This will help to ensure that the country develops a workforce with the right skills and expertise that can help our citizens to take full advantage of the opportunities in cyberspace.

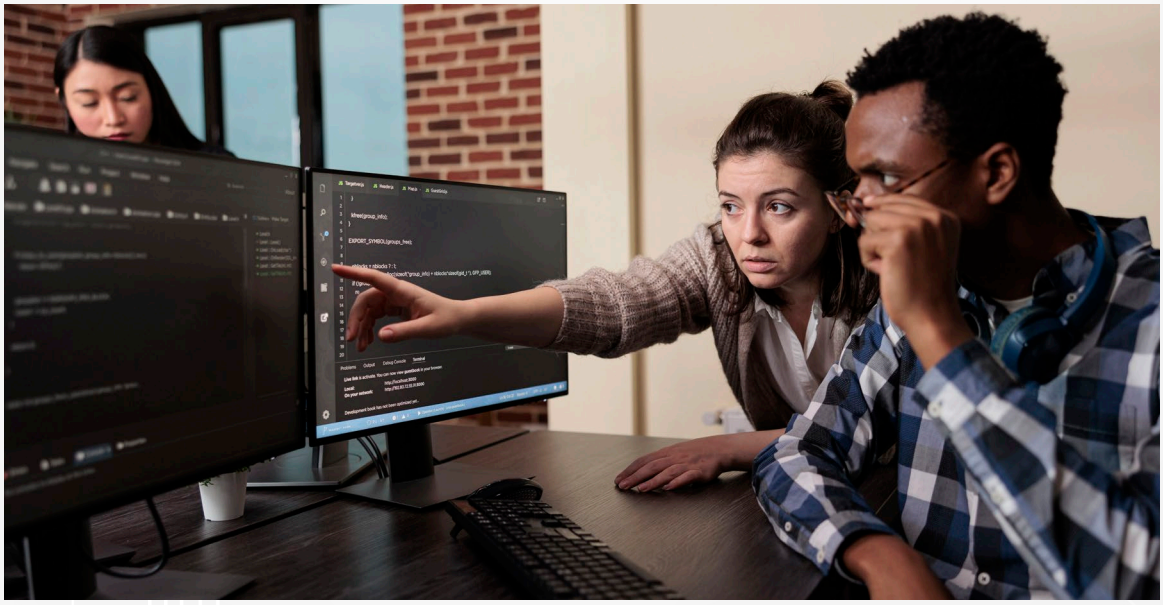
Pillar 3 – Promote Innovation, Enterprise Security and Cybersecurity Education (continued)

Objective 3: Build a Cyber Smart Nation

Increasing the understanding of cyber security risks and benefits is one of our strongest defenses. Engaging in cyber security awareness will ensure that our citizens are aware of online risks and know how to protect themselves.

To achieve these objectives, the following actions will be undertaken:

- Promote the development of capabilities in conducting cyber exercises;
- Promote the adoption and implementation of Information Security Standards and guidelines;
- Promote the adoption of cyber insurance within enterprises;
- Build capacity of local ICT professionals and the general workforce in cybersecurity;
- Inculcate Cybersecurity into the education system at primary, secondary and tertiary levels;
- Together with private sector, promote cybersecurity scholarships and sponsorships to attract promising students;
- Promote cybersecurity Research and Development (R&D) collaborations between the government, industry and academia;
- Encourage security firms to setup local and regional offices in Mauritius;
- Promote the development of local security products;
- Develop a National Child Online Safety Framework to address new cyber threats against children and young people; and
- Work with the private sector and international partners to raise awareness of the importance of cyber security across our community.



Pillar 4 – Strengthened Regional and International Partnership

Cyber security is an important issue for regional and international cooperation. Cyberspace is already a core foreign policy issue and a central theme of Mauritius diplomatic efforts. Developing norms of state behaviour, the application of international law, Internet governance and cyber innovation are regularly discussed at multilateral forums. Mauritius needs to strengthen its partnership regionally and internationally to focus on its security and economic interests. This strategy aims at building the nation's cyber security through stronger obligations and partnerships that will give us the best chance of disrupting or minimising sophisticated cyber threats.

The strategic objectives for a strengthened regional and international partnership are:

Objective 1: Strengthen and expand Mauritius strategic international cyber security partners and trusted networks

The lightning-fast speed of cyber-attacks requires quick and coordinated actions both at national and international levels. Mauritius will work closely with the international community and cybersecurity partners to further strengthen the platforms and procedures for reporting cyber incidents, sharing information and responding to possible breaches.

Mauritius will also partner with regional and international organisations to tackle cybercrime. Moreover, the network of CERT relationships could also be expanded by signing MoUs with other CERTs to enhance cyber incident reporting and response linkages.

To promote exchanges on current and emerging cybersecurity issues, Mauritius will continue to contribute to UN Processes such as Open Ended Working Group (OWEG), Group of Governmental Experts (GGE) and also to regional and international cybersecurity and cybercrime conferences, workshops, seminars and forums.

Pillar 4 – Strengthened Regional and International Partnership (continued)

Objective 2: Promote regional and international capacity building initiatives

Cyber threats are borderless and no country can deal with the rapidly evolving threat landscape alone. Mauritius stays committed to build cybersecurity capacity within the African region in operational, technical, legislative, cyber policy and diplomatic areas. Mauritius will focus on building understanding and raising awareness in these areas, as well as conducting training and exercises to raise capacity through its ITU Centre of Excellence.

To achieve the strategic objectives for a strengthened regional and international partnership, the following measures will be taken:

- Work closely with regional and international community and cybersecurity partners;
- Promote capacity building at the regional and international levels through online cybersecurity trainings and cyber drills;
- Expand the network of CERT relationship for collaboration on incident response and fighting against malicious activities through Memorandum of Understanding (MoUs) with international and regional CERTs such as CERT-India, Singapore CERT, Africa CERT, amongst others; and
- To promote cyber diplomacy to position Mauritius internationally by participating and contributing in different foras driven by regional and international agencies.

Pillar 4 – Strengthened Regional and International Partnership (continued)

Working with Regional and International Partners

International Conventions on Cybersecurity and Cybercrime

- Mauritius acceded to the Budapest Convention on Cybercrime in October 2013
- Mauritius ratified to the Malabo Convention (African Union Convention on Cybersecurity and Personal Data Protection) in 2017.

Regional and International Alliances

- Mauritius is member of the African Union, SADC, COMESA, IOC, IORA
- Mauritius signed the Commonwealth Cyber Declaration in April 2018
- It is party to many fora and alliances such as :
    - Forum of Incident Response and Security Teams (FIRST)
    - Cybersecurity Alliance for Mutual Progress (CAMP)
    - Global Forum for Cyber Expertise (GFCE)
    - Global Action against Cybercrime Extended Project (GLACY/ GLACY+)
    - Cyber Resilience for Development Programme of European Union (Cyber4Dev)
    - MoU with the Government of Estonia and Seychelles in the field of ICT

Assistance to the African Region

CERT-MU provided assistance to the following neighboring countries:

- Assisted Rwanda CERT in 2022 for its FIRST Affiliation.
- Assisted the Zambia CERT in 2017 for its FIRST Affiliation.
- Assisted Senegal for the concept development of setting up the Senegalese national CERT, following request of the Council of Europe.
- Assisted Tonga, Madagascar, Ivory Coast, and Philippines on their study tour for the set-up of their National CERTs.

GOVERNANCE FRAMEWORK AND RESPONSIBILITIES

Governance Framework and Responsibilities

The Government recognises the importance of effective strategy implementation. This requires a structured governance framework that has been established into the new Cybersecurity and Cybercrime Act 2021 in the form of a National Cybersecurity Committee. The said committee has a wider membership from across the sectors, including the private sector and the civil society.

The committee consists of 13 members from the following institutions, including a Chairperson:

- MITCI
- Prime Minister's Office
- CERT-MU
- Data Protection Office
- Attorney General's Office
- Mauritius Police Force
- Regulatory Bodies (ICTA, FSC, BoM)

Governance Framework and Responsibilities (continued)

The roles and responsibilities of the Stakeholders towards this collaborative framework are as follows:

Stakeholders	Role(s) and Responsibilities
National Cybersecurity Committee	• Coordinate and facilitate the implementation of the National Cybersecurity Strategy. • Advise the Government on cybersecurity and cybercrime; • Implement Government policy relating to cybersecurity and cybercrime; • Coordinate all matters relating to cybersecurity and cybercrime; • Receive and act on reports relating to cybersecurity and cybercrime; • Coordinate and facilitate the implementation of a critical information infrastructure protection framework; • Coordinate the collection and analysis of internal and external cyber threats, and response to cyber incidents that threaten the Mauritian cyberspace; • Cooperate with computer incident response teams and other relevant bodies, locally and internationally, on response to cyber threats and cybersecurity incidents; • Establish cybersecurity best practices and standards for critical information infrastructures; • Promote capacity building on the prevention, detection and mitigation of cyber threats.

Governance Framework and Responsibilities (continued)

The roles and responsibilities of the Stakeholders towards this collaborative framework are as follows:

Stakeholders	Role(s) and Responsibilities
CERT-MU	The responsibilities of the National CERT will be: • To handle and coordinate cyber security incidents of national significance. • 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. • To steer the recommendations of the National cybersecurity committee related to cybersecurity and cybercrime. • To act on the recommendations of the NCC on the mitigation of critical cybersecurity incidents impacting critical information infrastructures as well as to advise NCC on the compliance of the periodical IT Security Audit conducted by CIIs.

Governance Framework and Responsibilities (continued)

The roles and responsibilities of the Stakeholders towards this collaborative framework are as follows:

Stakeholders	Role(s) and Responsibilities
Prime Minister's Office (PMO)	• The representatives of the PMO would be the PMO Security Division and their roles will be to advise and support the implementation of the strategy geared towards protecting Mauritius from cyber threats and attacks.
Ministry of Information Technology, Communication and Innovation	• Acts as the project owner and is responsible for taking up the necessary measures for successful implementation of the National Cybersecurity Strategy.
Mauritius Police Force	• The role of the Mauritius Police Force will be to enable effective prevention, investigation, and prosecution of various aspects of cybercrime, including critical operations.
Data Protection Office	• The Data Protection Office will act as the advisory body on data protection and privacy issues.
Civil Society	• The role of civil society will be to advise NCC on cybersecurity issues impacting communities as well as on the secure Internet infrastructure and services, including its best practices.

Governance Framework and Responsibilities (continued)

The roles and responsibilities of the Stakeholders towards this collaborative framework are as follows:

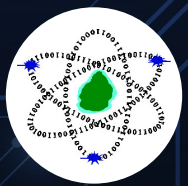
Stakeholders	Role(s) and Responsibilities
Regulatory bodies	The roles of the regulatory bodies will be to: • Establish, control, inspect and enforce regulations with regard to cyber security in line with the provisions of the Cybersecurity and Cybercrime Act 2021. • Encourage organisations to adopt security best practices and guidelines based on the established cybersecurity standards.
AGO	• The Attorney General's Office will provide legal advice and support in the investigation and prosecution of resolution of cybercrime matters.
Private Sectors	Private Sectors will be represented through respective associations. Their responsibilities will be to: • To advise NCC on secure products, services and architecture which are critical to the information infrastructure operators and for the general use. • To provide patches and mitigation strategies in the face of attacks. • To advise organisations and the general public on the use of cybersecurity best practices and guidelines.

ACRONYMS

- AGO – Attorney General's Office
- CAMP - Cybersecurity Alliance for Mutual Progress
- CERT-MU – Computer Emergency Response Team of Mauritius
- COE – Centre of Excellence
- COMESA -Common Market for Eastern and Southern Africa
- FIRST – Forum of Incident Response and Security Teams (FIRST)
- GFCE – Global Forum on Cyber Expertise
- GLACY – Global Actions on Cybercrime
- GLACY+ - Global Action against Cybercrime Extended Project
- ICTA - Information and Communication Technologies Authority of Mauritius
- ISO – International Organization for Standardization
- ISP – Internet Service Providers
- IOC – Indian Ocean Commission
- IORA – Indian Ocean Rim Association
- ITU - International Telecommunications Union
- ITSU – IT Security Unit
- IJLS - Institute for Judicial and Legal Studies of Mauritius
- MAUCORS – Mauritian Cybercrime Online Reporting System
- MDPA – Mauritius Digital Promotion Agency
- MITCI – Ministry of Information Technology, Communication and Innovation
- MRIC - Mauritius Research and Innovation Council
- MOETEST - Ministry of Education, Tertiary Education, Science and Technology
- MOFARIIT – Ministry of Foreign Affairs, Regional Integration & International Trade
- MOFED – Ministry of Finance, Economic, Planning and Development
- MOGECDFW – Ministry of Gender Equality, Child Development and Family Welfare
- ODPP – Office of the Director of Office Prosecutions
- PSEA – Private Secondary Education Authority
- SEDEC – Service Diocésain de l'Education Catholique
- SADC - Southern African Development Community
- SOC – Security Operations Centre
- SME – Small and Medium Enterprises
- UN OEWG – United Nations Open-Ended Working Group
- UN GGE – United Nations Group of Governmental Experts

NATIONAL CYBERSECURITY STRATEGY 2023-2026

For a **more secure** and **resilient Mauritius**



Computer Emergency Response Team of Mauritius