The ICT Sector is evolving rapidly, generating considerable areas of risks, which need to be addressed. Critical systems housed by the Police are protected both in their physical environment through isolation and segregation of networks and through layers of protection (access, roles and responsibilities, etc). Moreover, adequate controls are periodically reviewed to ensure their effectiveness.

The Social media is a powerful means of communication and enjoyment, if properly used. However, it has been noted that much damage is being caused by the messages and posts of a harassing nature.

Due to the rules of right to privacy and freedom of expression, communication which already exist between Law Enforcement Agencies (Police) and Social Media Houses are not of much, not to say any, help. Consequently, aggressive campaigns must be conducted by all stakeholders to enhance the level of awareness from school goers to the elderly.

Relevant information is being provided on the topics listed below in the ensuing paragraphs;

(a) General appreciation of the issues of information security
(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;
(c) The content of the concepts mentioned in paragraph 3 of the resolution A/RES73/27 and paragraph 2 of resolution 73/266;
(d) Possible measures that could be taken by the international community to strengthen information security at the global level;

1. General Appreciation of Issues of Information Security

Information is categorized in the Government Sector in line with the Government Security Instructions (GSI), which is a document issued by the Prime Minister's Office. This document also covers procedures for the upkeep of Information (Soft, Hard, Safe, etc.). The Police is also governed by the
Police Standing Orders in dealing with information security.

While information is disseminated on a 'Need to Know' basis, all Government officers have signed the 'Official Secrets Act' to ensure non-disclosure of information to unauthorized persons. This is binding even after the retirement of the officer from the service.

The Mauritius Police Force (MPF) has established a Police IT Unit in Year 2000 to monitor the deployment of IT related projects in the MPF; in Year 2005 a Digital Forensic Laboratory was set up in the Unit for the search, seizure, acquisition, examination and preservation of digital evidence and the generation of reports. Moreover, The MPF can rely on the various networks established, namely Interpol, the Points of Contacts under the Budapest Convention and the G 7 Network. With the wide experience of the above partners in the field of ICT security, their expertise may be sought to build capacity at the level of the Mauritius Police Force.

2. **Efforts to strengthen Information Security at National Level**

2.1 **Legal Instruments**

The following **legal instruments** relating to Information Security at National level have been reviewed and strengthened:

- Cybercrime Misuse Cybercrime Act 2003 (CMCA)
- The Data Protection Act 2017
- Computer Misuse and Cyber-Crime Act 2003
- Postal Services Act 2002 (as amended)
- The Information and Communication Technologies Act 2001 (as amended)
- The Electronic Transaction Act 2000 (as amended)
- Independent Broadcasting Authority Act 2000 (as amended)
Established legal framework concerning Cyber security and Cybercrime


- Currently, Computer Misuse and Cybercrime Act 2003 is being aligned with both the Budapest Convention on Cybercrime and the Malabo Convention on Cyber security and Personal Data Protection, of which Mauritius is a signatory.

2.2 Setting up of Units and Mechanisms

Various strategies have been put in place by the Ministry of Technology, Communication and Innovation (MTCI) from which the Mauritius Police Force (including the Police IT Unit) benefits, for example, the setting up of several units and mechanisms, namely;

a) The Mauritius Police Force has established a **Police Information Technology (IT) Unit in year 2000 and a Cyber Crime Unit in year 2006** to assist in the investigation of cybercrimes as provided for breaches of the main ICT Acts and to help in the computerization of the Police Department. The Police IT Unit operates with full respect for human rights and fundamental freedoms as guaranteed in the Constitution of Mauritius.

b) **Setting up of the IT Security Unit in August 2004** under the Ministry of Information Technology Telecommunications to act as a key contact point for IT Security in Government. It is also mandated to conduct comprehensive IT security risk assessment and risk management and IT security audits of information system infrastructures. It also carries out ongoing capacity building and awareness of officers and the public at large in the field of IT security for better preparedness to counter malware-related and criminal activities. IT security audits of information system infrastructures at Government and public sector
critical information infrastructures are also part of the IT Security Unit's responsibilities.

c) **Setting up of the Computer Emergency Response Team of Mauritius (CERT-MU)** in May 2018 to handle and coordinate information security issues at the national level. CERT-MU is a national CERT and operates under the umbrella of the National Computer Board, a parastatal body operating under the aegis of the Ministry of Technology, Communication and Innovation.

d) **Setting up of the Data Protection Office** in 2009 following the enactment of the Data Protection Act 2004. Mauritius was the first African country to ratify Convention 108 in June 2016 and amendments were brought accordingly to the Data Protection Act in order to be in line with EU standards. The new Data Protection Act 2017 was proclaimed in January 2018. It incorporates international best practices in data protection and is aligned with the European Union General Data Protection Regulation (GDPR).

e) **Setup of the Government Security Incident Response Team (G-SIRT)** in 2016, to respond effectively to ICT Security incidents counter cyber threats effectively. The G-SIRT has implemented an Automated ICT Security Incident Handling System (AISIHS) for better tracking and timely resolution of incidents.

f) **Setup of the Mauritian Cybercrime Online Reporting System (MAUCORS)** in 2018 to coordinate and resolve cybersecurity incidents effectively. The collected incident data is then used to analyse incident trends for carrying out risk profiling. The system is centralized and allows different stakeholders including CERT-MU, the Mauritius Police Force, the Data Protection Office, and Information and Communication Technologies Authority to log into, investigate on reported incidents and take actions accordingly. MAUCORS can be accessed on: [http://maucors.govmu.org](http://maucors.govmu.org)
g) **Setup of a National Disaster Cyber security and Cybercrime Committee** at the level of the Ministry of Technology Communication and Innovation to manage major cyber security threats and attacks.

h) **Crime Occurrence Tracking System (COTS)** is operational since December 2012 and covers 84 police stations across the island. The Crime Occurrence Tracking System (COTS) is used by the Mauritius Police Force - COTS caters for the end-to-end automation of all processes from the electronic lodging of a complaint at a Police Station to its determination in a court of law with the possibility of electronic tracking of intermediate phases.

i) **Setup of a Regional Centre of Excellence on Cybersecurity and Cybercrime**
Mauritius is setting up a Regional Centre of Excellence on Cybersecurity and Cybercrime. It will act as a regional centre and its role will be to set out a right approach to fight cybercrime through improved law enforcement capability, effective criminal justice framework and active international engagement. The focus areas are harmonization of legislation, capacity building and international cooperation.

2.3 **Other Measures**

2.3.1 **Development of a National Cyber Incident Response Plan**

Mauritius has developed a National Cyber Incident Response Plan which seeks to provide advice and discuss the actions and responsibilities for a coordinated and multidisciplinary approach to cyber threats and security incidents.

This will help to respond and recover from cyber security incidents of national significance impacting critical systems and the economy.

2.3.2 **Safe City project**

The implementation of the Safe City project has started in January 2018. It includes
ICT systems which aim at making the country safer for its citizen by acting as a deterrence as well as to providing means to track criminals/suspects. It comprises a CCTV Smart Camera Surveillance System with more than 4000 cameras across the island, a Multimedia Radio Trunking System, a Central Watch and Management System, an Integrated Emergency Response Management System and an Intelligent Command System, to enable the Police Department to obtain better intelligence with a view to optimizing response.

2.3.3 Fire Arms Index Management System

A Fire Arms Index Management System has been set up in 2008. It helps to manage and keep track of licenses which have been issued for the use of firearms.

2.3.4 Passport and Immigration System

The Passport and Immigration System has been implemented at the Passport & Immigration Office (PIO) and is operated to ensure the effectiveness of border control management. The system includes a Border Control module which facilitates management of all entry and exit points in Mauritius and provides real time information on citizens and foreigners entering or leaving the country. In addition, an Advance Passenger Information system is currently being implemented at the PIO.

Data regarding passengers will be made available by foreign airlines to PIO and law enforcement agencies like Customs, Anti-Drug and Smuggling Unit, National Security Service, Central Investigation Division and Counter Terrorism Unit. In this way, the latter will be able to automatically scrutinise passengers of interest in a systematic manner prior to their arrival. The relevant authorities will be alerted of known criminals, terrorists or controversial individuals travelling to the country.

2.4 Development of national strategies and Policies

- Mauritius has established the National Cyber security Strategy and the National Cybercrime Strategy in 2014 and 2017 respectively. The National Cyber Security Strategy provides an overview of what it takes to effectively protect information systems and networks and gives an insight into the Government's approach and
strategy for protection of cyberspace in the country. On the other hand, the National Cybercrime Strategy sets out the Government's approach to fight cybercrime through improved law enforcement capability, effective criminal justice framework and active international engagement.

- The Digital Mauritius 2030 Strategy was released in December 2018. It proposes to tackle cybercrime by strengthening legal frameworks, maintain strong cyber security mechanisms through regional and international linkages and educate local communities on cyber security for a safe and secure cyber space.

- The country is also developing the Critical Information Infrastructure Protection (CIIP) Policy to better respond to information security incidents impacting critical information infrastructures.

3. Comments in relation to the UNGA Resolutions 73/27

Para 1.1. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

Mauritius ratified the Budapest Convention in Year 2013, yet the Cybercrime Misuse Cybercrime Act (CMCA) was promulgated in Year 2003 and is in harmony with the Budapest Convention.

Para 1.2. States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated. In case of ICT incidents, States should consider
all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

The **Extradition Act 2017** provides, subject to specific conditions, for suspects arrested in Mauritius to be extradited for offences committed in a foreign country where they could be required to face justice.

The **Mutual Legal Assistance Act 2003** is also a legal instrument which is available, inter alia, to require suspects and detainees to continue to serve imprisonment in their country of origin.

The CMCA 2003 also provides for Service Providers to preserve evidence upon the Order of a Judge which may be secured on application by way of affidavit.

**Para 1.3. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts.**

The Information and Communication Technologies Authority (ICTA) is responsible to speak up and report concerns about the ICT regulatory frameworks and laws, and seek clarification and guidance where there is doubt.

The 'Child Sexual Abuse Filtering' implemented by ICTA is one such example.

**Para 1.4. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.**

As stated above, the CMCA 2003 provides for Judge's Order to be sought to direct service providers and custodians of information to preserve evidence.
The authorities may also have recourse to the **Mutual Legal Assistance (MLA)** for access to information which eventually is used as evidence in a court of law.

The Budapest Convention List of Contacts, the G-7 List of Contacts and the Interpol Network are other avenues which the MPF may actually have recourse to.

It is proposed that court sittings may be held through video conferencing in cases where the jurisdiction and the other parties are remote.

*Para 1.5. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 of 5 July 2012 and 26/13 of 26 June 2014 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.*

The Constitution of Mauritius provides for freedom of expression, right of access to information, privacy among other rights.

*Para 1.6. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.*

Mauritius is a democratic country where the rule of law prevails.

*Para 1.7. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 of 23 December 2003 on the creation of a global culture of cyber security and the protection of critical information infrastructures, and other relevant resolutions.*

A **cyber security strategy** has been set up since 2013 by the Ministry of Technology,
Communication and Information (MTCI) and adopted by the Government Sector, including the Police with objectives, inter-alia, to secure the cyberspace and establish a front line defense against cybercrime, enhance resilience to cyber-attacks.

Critical infrastructure as the Government Online Centre (GOC) hosting Government IT Systems and Websites, the Cyber Towers, Police and Health Institutions, Government and Financial sectors and many more are all subject to the need for protection.

Measures and strategies have been spelt out at 2 above.

**Para 1.8 States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.**

Input is at 1.4. above under paragraph 3.

**Para 1.9. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.**

Law Enforcement Agencies (LEAs) have well established Standard of Operating Practices (SOPs) to ensure integrity of the supply chain.

In addition to the Government Security Instructions, the Police IT Unit also complies with the Police Standing Orders to that effect.

All prospective bidders in tenders for ICT Systems have to comply to stringent information security measures embedded within the specifications to ensure that these systems, once implemented, contain adequate controls.

**Para 1.10. States should seek to prevent the proliferation of malicious ICT tools and**
techniques and the use of harmful hidden functions.

At national level, the Computer Emergency Response Team (CERT-MU) is responsible for the prevention of proliferation of malicious ICT tools and techniques. The Police IT Unit receives communiques from the CERT-MU whenever such incidents occur.

Furthermore, the Government Sector, including the Police IT Unit makes use of licensed Anti Viruses and Anti Malwares to secure its systems.

The Police IT Unit is contemplating to adhere to the requirements of the ISO 27001:2013 for an Information Security Management System. Initial Audits by external parties have already been conducted.

Para 1.11. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies for such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

A mechanism exists whereby all ICT vulnerabilities are reported to the CERT -mu for investigation and remedial action.

Para 1.12. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

This is taken on board by the CERT-MU Unit.

Para 1.13 States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behaviour in
information space with regard to their potential role.

The Police IT Unit, together with the Cybercrime Unit, conducts awareness sessions regularly through official trainings, fairs, workshops and other means to reach out to members of the private sector and the civil society to improve security on and the use of ICTs.

4. Possible Measures to strengthen information security at the global level

4.1 The following measures may strengthen information security at global level:

a) Mauritius has been selected as the ITU Centre of Excellence in the focus area of Cybersecurity training in the region.

b) The EU Cyber Resilience for Development Programme (Cyber4D) has been started by European Union in March 2018 with an aim to increase the security and resilience of critical information infrastructure and networks supporting the critical services of third countries. As part of this project, European Union has included Mauritius as one of the priority countries in East Africa. Mauritius' role in this programme will be one of a model cyber resilience country to showcase its experience and best practices in East Africa.

c) Urgent need for cooperation/joint operations among states at international level and regional level (INTERPOL, SADC SARPPCCO, COMESA, African Union Commission and COI) and for working together to mitigate threats such as cybercrime, cyber-attacks on critical infrastructure, electronic espionage, bulk data interception which could precipitate massive economic and societal efforts.

d) Greater participation of Governments, and experts from academic and civil society in international and regional forums to support/share their knowledge on proven solutions and to develop cyber policies/rules/laws based on best practices.
e) States should not knowingly allow their territory to be used for internationally wrongful cyber acts and should not conduct or knowingly support ICT activities that intentionally damage critical infrastructure and encourage the spread of cyber-attacks.

f) As a matter of information, between 2015 to year 2018, a total of forty-nine (49) Police Officers of all ranks have attended courses/Committees/workshops/Conferences on Cyber Security and Cyber Crime Investigation Training overseas.

g) Attending international fora, where proven solutions could be shared and learnt in specific issues would be a good initiative. Further, Joint Operations with friendly countries in the region (E.g. SADC Countries) should be encouraged as well as participation in cybercrime and cyber security drills involving transnational stakeholders in international meetings on the subject in order to learn the best practices and share experience.

h) Memoranda of Understanding (MoU) have been signed with CERT Japan, CERT India and Symantec to build capacity on cyber security/cybercrime and to resolve incidents quickly. Mauritius has also signed an MoU with Estonia to promote awareness building on cyber security and protection of critical infrastructure.

i) Mauritius has signed the Commonwealth Cyber Declaration at the Commonwealth Heads of Government Meeting (CHOGM) held in April 2018 in London and is committed to implement the recommendations of the Declaration.

j) Mauritius being a member of Southern African Development Community (SADC), Common Market for Eastern & Southern Africa (COMESA) is a vivid example of the South-South African Cooperation. In April 2016, the Ministry of Technology, Communication and Innovation organised a regional cybersecurity drill in collaboration with the International Telecommunication Union (ITU) for African countries to assess the organisation's readiness to face cyber threats and respond appropriately. A similar drill was organised in September 2018 for SADC
4.2 Part of international fora and alliances

a) Mauritius is a party to many fora and alliances such as the Forum of Incident Response and Security Teams (FIRST), Cybersecurity Alliance for Mutual Progress (CAMP) and Global Action against Cybercrime Extended Project (GLACY+) of the Council of Europe. GLACY+ is a Joint project of the European Union (Instrument Contributing to Peace and Stability) and the Council of Europe. GLACY+ is intended to extend the experience of the GLACY project (2013 - 2016) and supports twelve priority and hub countries in Africa, Asia-Pacific and Latin America and the Caribbean region - Cabo Verde, Chile, Costa Rica, Dominican Republic, Ghana, Mauritius, Morocco, Nigeria, Philippines, Senegal, Sri Lanka and Tonga. These countries may serve as hubs to share their experience within their respective regions. GLACY+ aims to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.

b) FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactively as well as proactively. FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. Currently FIRST has more than 400 members, spread over Africa, the Americas, Asia, Europe and Oceania.

c) The Cyber security Alliance for Mutual Progress (CAMP) is initiated by the Korean government with the purposes of achieving sustainable benefits and serving as a platform where members prepare themselves with collective actions to keep cyberspace safe. CAMP serves as a network platform to lift up the overall level of cyber security of the members. The members share development experiences and
trends of cyber security to catalyze mutual growth as well as contribute to development of global cyber security for large.

4.3 Accession to Budapest Convention on Cybercrime

- Mauritius has acceded to Budapest Convention on Cybercrime in October 2013 and is one of the priority countries of the GLACY+ project of the Council of Europe.

4.4 Ratification of AU Convention or Malabo Convention on Cyber security and Personal Data Protection

- Mauritius has ratified the AU Convention on Cyber security and Personal Data Protection in March 2018.

4.5 Proposals to strengthen information security at the global level:

- Creation of a pool of skilled cyber security professionals to serve the region
- Setting up of the Public and Private Partnership platform
- Establishment of efficient communication channel with the regional countries
- Formalisation of Mutual Legal Assistance (MLA) with the regional countries
- Major references to reports from the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security have been made in the resolution documents. Time-permitting, access to these documents and their inherent provisions could be required for more detailed proposals.
- The Ministry could look into requesting participation in these forums for gaining expert information as well contributing to the body of knowledge in these fields given the relatively good rating of Mauritius in the Cyber security Index and other related indices
- The resolution places emphasis on not supporting malicious activity from member states. Mauritius could make a claim that it does not engage in malicious activity on its territory indicating the measures taken to prevent such nefarious activities.
- Establish CERT-MU as a legal entity and as a body providing cyber security services at national and international level through partnerships
• Conduct cyber security threat assessment exercises for improved cyber threat preparedness
• Issue guidelines on good cyber security practices
• Set-up of a regional capacity building centre for cybercrime for enhanced cyber maturity in the African region.
• Formulate a National Cyber Security Accreditation Framework for regional countries
• Promote Mauritius cyber security services in the region