Jamaica

Last Updated: September 2020

CYBERSECURITY POLICY

Strategy Documents

Jamaica National Cyber Security Strategy
Ministry of Science, Energy & Technology

Four key areas:

1. Technical measures: resilient critical infrastructure; national capability for ensuring timely and effective response to cyber incidents; a risk-based approach in establishing IT and information security standards, policies and guidelines for ICT infrastructure and cybersecurity governance; leveraging regional and international partnerships;
2. Human resource and capacity building: pool of skilled and knowledgeable professionals;
3. Legal and regulatory: safe place to do business; establishment of a robust governance framework to support the cyber security landscape; maintenance of an effective legal framework and enforcement capabilities to investigate and prosecute cybercrimes; legal protection in cyberspace;
4. Public education and awareness: knowledge and awareness of cyber risks and actions to be taken regarding cyber security; implementation of measures to protect vulnerable groups in cyberspace, cyber security culture.

Source Source 2

28 January 2015

STRUCTURE

National Centre or Responsible Agency

Information Communication Technology Division
Ministry of Science, Energy & Technology
Tasked with, inter alia, policy development in relation to Cybersecurity and Internet Governance and implementation of a National Computer Incident Response Team/Cyber Emergency Response Team.
Source

Key Positions

Principal Director, Information and Communication Technology

Ms. Kaydian Smith is the Principal Director for Information Communications Technology in the Ministry. Under the Direction of the Chief Technical Director, ICT, her responsibilities include:

- Guiding the reform of the current Telecommunications Act with a view to developing a robust omnibus ICT Legislation.
- Guiding the development of a Free and Open Source Software Policy for use across Government Ministries, Departments and Agencies; and
- Supervision of Directors with responsibility for, policy development in relation to Cybersecurity and Internet Governance and implementation of a National Computer Incident Response Team/Cyber Emergency Response Team.

Jamaica

Last Updated: September 2020

Source

Head, Information Communication Technology Division
Ministry of Science, Energy and Technology
Source

Dedicated Agencies and Departments

National Cyber Security Task Force
Government of Jamaica

- Comprises a wide cross-section of stakeholders from the public and private sector, as well as academia;
- Tasked with: formulating a strategy to develop, grow and retain high quality cyber talent for the national workforce; assisting in creating a framework to facilitate the building and enhancement of confidence in the use of cyberspace and the protection and security of related assets through collaboration amongst all stakeholders; and establishing a public education and awareness programme.

Source

Communications Forensics and Cybercrime Unit
Jamaica Constabulary Force
Provides support for the investigation fo crimes.
Source

December 2010

Digital Evidence and Cybercrimes Unit
Office of the Director of Public Prosecution

Established with a view to:

- Conducting in-depth research, preparation and prosecution of cybercrimes and cases involving digital evidence; and
- Providing advice to the police and clerk of courts with regards to the preparation and prosecution of cybercrimes, as well as cases, involving digital evidence.

Source

2009

National CERT or CSIRT

CIRT Jamaica
Ministry of Science, Energy & Technology

Responsible for:

- Creating a framework to build and enhance confidence in the use of cyberspace, with a view of advancing Jamaica’s economic interests and maintaining national security under all conditions;
- Coordinating cyber-related incident response, timely recovery from incidents, rapid distributions of advisories and alerts within the Government;
- Continuous monitoring of threats to the Government's IT resources.

Source

January 2016 (reported on)

Jamaica

Last Updated: September 2020

LEGAL FRAMEWORK

Legislation

The Cybercrimes Act of 2015

The Cybercrimes Act of 2015 repealed and replaced the Cybercrimes Act of 2010. The new act incorporates new offences. It especially attempts to counter the use of computers for malicious communication or cyber bullying.

Lists offences, including:

- Unauthorised access to computer program or data;
- • Access with intent to commit or facilitate commission of offence;
- Unauthorized modification of computer program or data;
- Unauthorized interception of computer function or service;
- Unauthorized obstruction of operation of computer;
- Computer related fraud or forgery;
- Use of computer for malicious communication;
- Unlawfully making available devices or data for commission of offence;
- Offences relating to protected computers;
- Inciting;
- Offences prejudicing investigation;
- Offences by bodies comrporate.

Source

2015

COOPERATION

Bilateral and Multilateral Cooperation

Cooperation, OAS-Jamaica

Ministry of Science, Energy & Technology

Cooperation with OAS (Inter-American Committee against Terrorism) to:

- Elaborate a National Cybersecurity Strategy;
- Develop a roadmap for the establishment of a CSIRT.

Source

16 September 2014

Membership

- **Caribbean Community (CARICOM)**
- **Commonwealth**
- **International Telecommunications Union (ITU)**
- **Organization of American States (OAS)**
- **United Nations (UN)**