# NATIONAL CYBER SECURITY STRATEGY

GOVERNMENT OF **JAMAICA**

# TABLE OF CONTENTS

# ACKNOWLEDGEMENT

The Jamaican National Cyber Security Strategy was developed with the technical support of the Cyber Security Program of the Organization of American States (OAS). This effort was made possible thanks to the financial contributions of the Governments of Canada, the United Kingdom, and the United States of America. Several other organizations provided their input and guidance into this project including, among others, the Commonwealth Cybercrime Initiative, the Commonwealth Telecommunication Organization, and the Global Cyber Security Capacity Centre of University of Oxford.

# LIST OF ACRONYMS

Bring Your Own Device (BYOD)

Business Process Outsourcing (BPO)

Communication Forensics and Cybercrime Unit (CFCU)

Cyber Incident Response Team (CIRT)

Government of Jamaica (GOJ)

Industrial Control Systems (ICS)

Information and Communications Technology (ICT)

Information Technology (IT)

International Telecommunications Union (ITU)

Internet of Things (IoT)

Jamaica Constabulary Force (JCF)

Jamaica Information Service (JIS)

Micro, Small and Medium Enterprises (MSMEs)

Ministry of Education (MOE)

Ministry of Finance and Planning (MOFP)

Ministry of Foreign Affairs and Foreign Trade (MFAFT)

Ministry of Health (MOH)

Ministry of Justice (MOJ)

Ministry of Labour and Social Security (MLSS)

Ministry of National Security (MNS)

National Cyber Security Task Force (NCSTF)

Office of Director of Public Prosecution (ODPP)

United Nations Office of Drugs and Crime (UNODC)

Universal Service Fund (USF)

# EXECUTIVE SUMMARY

This Strategy recognizes that Information and Communications Technology is a necessary tool for national development but with it comes inherent risks which must be mitigated against. Cybercrimes have the potential to erode confidence and trust in the economy thereby impairing national development.

This Strategy seeks to establish a framework built around the following key areas: i) Technical Measures; ii) Human Resource and Capacity Building; iii) Legal and Regulatory; and (iv) Public Education and Awareness.

## NATIONAL CYBER SECURITY FRAMEWORK


**Figure 1.** National Cyber Security Strategy Objectives

**Technical Measures** will seek to ensure that network infrastructure and in particular critical infrastructure systems are resilient to cyber threats. These efforts will include the establishment of a Cyber Incident Response Team (CIRT). A risk based approach will be adopted whereby risk assessments will be undertaken and the necessary preventative measures (including the application of best practices and standards) will be promoted and adopted by both the private and public sector.

**Human Resource and Capacity Building** recognises that establishing and sustaining a pool of trained professionals in Information Security will assist in ensuring there is national capacity to detect, respond and recover from cyber incidents as well as promote local research and development in Information Security in Jamaica.

**Legal and Regulatory** efforts will be focused on examining and undertaking reform in the legislative landscape to promote a healthy and safe business environment where businesses can thrive and all stakeholders can be assured that should they fall victim to cybercrimes there is recourse.

**Public Education and Awareness** seeks to develop targeted campaigns to facilitate each stakeholder group's understanding the potential threats and risks they would likely face and appropriate action they can take to protect themselves. The vulnerable in the society are specifically i**dentified as requiring special attention.**

**This Strategy** therefore represents a high-level approach to cyber security that establishes a range of national objectives and priorities that will be achieved within a specified timeframe[1]. The Strategy seeks to:

- a and awareness regarding cyber security; and
- develop a culture of cybersecurity.

Ultimately the Strategy, will seek to engender confidence in cyber space such that Jamaicans can continue to achieve their full potential.

---

1. ENISA National Cyber Security Strategies Practical Guide on Development and Execution-December 2012

# INTRODUCTION

# INTRODUCTION

Since the liberalization of the Telecommunications sector in 1999, phenomenal strides have been made in the area of Information and Communications Technology (ICT). Jamaica now boasts tele-density in excess of 108%; a 100% digital telecommunications network; submarine fibre optic transmission ring around the island; international submarine cable links from Jamaica to Cayman, the Dominican Republic, Cuba and Florida; and a competitive ICT sector.

An additional outcome of liberalization has been the growth of the Business Process Outsourcing (BPO) sector. Jamaica has become a highly competitive and attractive business destination and a leading contact centre location in the English-speaking Caribbean. As at March 2014, the local ICT/BPO industry is estimated to be valued at US$230 million, accounting for six per cent of the Caribbean and Latin American market. Additionally, there are 36 ICT/BPO operations employing over 14,000 individuals in the industry and is poised to double in size by 2016 .

While Jamaica's tele-density indicates universal access to voice telephony, internet penetration and more specifically fixed broadband penetration remains low at 4.4% in 2013. Through the Universal Service Fund (USF) the Government has and is utilizing various strategies to encourage access including the:

- establishment of Community Access Points (a total of 181 to date);
- establishment of an island-wide broadband wide area network connecting secondary schools, libraries and select post offices and health facilities; and
- deployment of technology in schools through the eLearning and the Tablets in School Projects.

Additionally, it is expected that more consumers will have access to broadband with the grant of a licence for the use of the 700 MHz spectrum for mobile broadband deployment.

**LOCAL ICT/BPO INDUSTRY** IS ESTIMATED TO BE VALUED AT **US$230** MILLION

**06%** OF **THE CARIBBEAN** AND **LATIN AMERICAN** MARKET

**36** **ICT/BPO** OPERATIONS **BY 2016** IS POISED TO **DOUBLE** IN SIZE

2. Doing Business in Jamaica's Knowledge Services Sector, JAMPRO, March 2014

**INTERNET** HAS

**50**

**BILLION**

**CONNECTIONS**

[APPROXIMATELY]

BY **2020**

IT IS PREDICTED TO

**INCREASE** TO

**13**

**QUADRILLION**

The result of the foregoing is that Jamaicans are and will continue to be more connected to each other and to the world. However, with increased connectivity and the growing phenomenon of the Internet of Things (IoT) come increased threats to the daily operations of individuals and businesses alike. In light of estimates indicating that the Internet has approximately 50 billion "things" connected to it, with the number of connections predicted to increase to 13 Quadrillion by the year 2020[3]; Jamaica must be prepared to address these threats if it is to continue to utilize ICTs for economic and social development.

## NATIONAL DEVELOPMENT AND THE ROLE OF ICT

The Government's vision with respect to ICT is to create a knowledge-based and educated society which is globally competitive and productive; giving rise to the strategic placement of Jamaica as the key ICT hub within the region'.[4]

Additionally, the **National Development Plan (Vision 2030)**[5] has as one of its national outcomes a technology enabled society where ICT, as a sector and an enabler of other sectors, is utilized to, among other things, drive productivity and efficiency and unleash the creative potential of Jamaicans.

At the centre of Jamaica's focus on increased use and application of ICT is broadband. Several authoritative and global research studies have clearly established the link between ICT use and GDP growth[6]. More recently, with broadband being considered critical to economic and social development, more and more studies have focused on elaborating this link. Research undertaken by the World Bank has shown that the development impact of broadband on emerging economies is greater than for high-income countries and that broadband has a potentially higher growth effect than other ICTs, including wireline telephony and mobile telephony[7].Additionally, research also suggests that broadband access and broadband speed positively affect household incomes[8] and that children with Internet access at home perform better in school and are better-protected against online dangers as they are usually under parental guidance[9].Jamaica is positioning itself to benefit from the increased use of ICTs and broadband and therefore notwithstanding potential security threats and the myriad of possible cyber-attacks, it cannot become complacent if it is to reap the derivative economic benefit inherent in utilizing ICTs. Tangible and workable solutions must be found to create a safe environment which engenders confidence in the use of ICTs by both citizens and businesses while enabling creativity and innovation.

**Children with Internet access** at home perform better in school and are **better-protected** against online dangers.

**Figure 2.** www.istock.com

3. CISCO 2013 Annual Security Report
4. Government of Jamaica, Information and Communications Technology (ICT) Policy, prepared by the Information and Telecommunications Department, Office of the Prime Minister, March 2011
5. Vision 2030-National Developmental Plan Accessed at http://www.vision2030.gov.jm/
6. David Dean et al., The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy, Boston Consulting Group, perspective 27 (January 2012).
7. Building Broadband: Strategies and Policies for the Developing World, International Bank for reconstruction and Development/. World Bank, 2010
8. Socioeconomic Effects of Broadband Speed– Ericsson, Arthur D. Little and Chalmers University of Technology, 2013
9. The Broadband Challenge, Broadband Commission for Digital Development, Geneva 2011

## THE THREAT OF CYBERCRIME AND ITS IMPACT ON NATIONAL SECURITY

The **National Security Policy**[10], states that 'a fight against crime is therefore a fight for development; measures to reduce the social and economic damage caused by pervasive crime have to be integral to the developmental activities of the state.' It is also a globally recognized fact that cybercrime is a real and present threat to the stability of any society and Jamaica is no exception. The scale and sophistication of cybercrime has caused many Governments to rethink their strategy in protecting their citizens in an increasingly technology driven and dependent global economy.

Cybercriminals usually have clear objectives when launching their exploits. They know what information they are seeking or what outcomes they want to achieve, and they know the path they need to take to reach these goals. These criminals will spend significant time researching their targets, often through publicly available information on social networks, and plan their objectives strategically. Many of these malicious attacks have sought to expose and/or exploit sensitive and confidential information which can have detrimental effects for government and critical infrastructure operators.

There is a thinking that users of the Internet should assume that nothing in the cyber world can or should be trusted. Yet organizations in the public and private sectors as well as individuals still desire the assurance that the technologies they rely on every day can be trusted[11].

In recent years increasing amounts of personal and sensitive data, such as names, addresses and credit card information, are being harvested by businesses. Additionally, increasing amounts of businesses store personal and sensitive data on online platforms or other electronic media. As massive amounts of data become readily accessible; they have become high commodity items to cyber criminals as they can be sold to other malicious actors. Consequently individuals, businesses and government alike must take adequate precautions to protect their data.

**Cybercrime is a real and present threat** to the stability of any society and Jamaica is no exception.

Global trends in cybercrimes demonstrate that the financial sector is the sector most targeted by cyber criminals. Their activities include phishing, identity theft and the creation of fake banking apps[12]. The United Nations Office of Drugs and Crime (UNODC) estimate that identity theft is the most profitable form of cybercrime, generating perhaps US$1 billion per year in revenue on a global basis. The same UNODC report estimated that the cost of identity theft using cyber techniques in the United States was US$780 million[13]. Additionally, Interpol has stated that more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities. These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, internet auction fraud, the penetration of

10. A New Approach: National Security Policy for Jamaica, 2014
11. 2014 CISCO Annual Security Report
12. Blurring Boundaries-Trend Micro Predictions for 2014 and Beyond, Accessed at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf
13. The Economic impact of Cybercrime and Cyber Espionage – Center for Strategic and International Studies, July 2013 (McAfee)

online financial services, as well as the deployment of viruses, botnets, and various email scams such as phishing[14].

It is becoming increasingly evident that organized international gangs are behind most Internet scams and that cybercrimes' estimated cost is more than that of cocaine, heroin and marijuana trafficking put together[15]. Criminal gangs have recognized that their exposure is less when they perpetrate cybercrimes with high profits as opposed to other traditional forms of organized crimes. Jamaica's National Security Policy therefore identifies cybercrimes as Tier 1- Clear and present danger, with a high impact and high probability of occurrence[16].

Another area often targeted by cybercriminals is critical infrastructure. The critical infrastructure national landscape is the bed rock of daily operations. The disruption of same has the potential to reduce the flow of essential goods and services, impede or impair important economic and financial operations, and fundamentally shut down the country. Therefore, limiting the vulnerability of critical infrastructure by applying relevant security standards, while at the same time assessing the risks, will reduce the options available to criminals to attack these systems.

## CYBER INCIDENTS IN JAMAICA

In Jamaica the emerging trend indicates an increase in cyber incidents. Figure I below shows cybercrimes for the years 2011 and 2012, while Figure II shows cybercrimes for the period January – August 2014. Figure III reflects cyber activities reported to the police for the years 2011 and 2012 but are not offences under the Cybercrimes Act.

In examining our cyber security approach, national security issues cannot be ignored. Therefore the necessary support needed for the police, intelligence and other national security services to, among other things, ensure the maintenance of law and order, to deter, mitigate and protect against significant external or internal threats, is critical. It will involve ensuring that vital infrastructure is bolstered and resilience is built into our social and economic systems so that they can withstand threats[17].

## FACING THE CHALLENGE

The Government is aware that facing the challenge will be difficult. The inherent nature of cybercrime makes it a new paradigm for law enforcement agencies. It is recognized that there are existing deficiencies in our capacity, processes and technology to properly investigate and prosecute these crimes. Additionally, it is recognized that the trans-border nature of cybercrime requires international cooperation to assist in the prosecution, mitigation and recovery efforts. In this vein, it is recognized that the academic community and private sector are critical stakeholders in securing our cyberspace and must play a significant role in advancing these efforts.

---

14. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
15. Norton Cybercrime Report 2011
16. A New Approach: National Security Policy for Jamaica, 2014, Pg. 10
17. Ibid. 7

## CYBERCRIMES FOR 2011 AND 2012

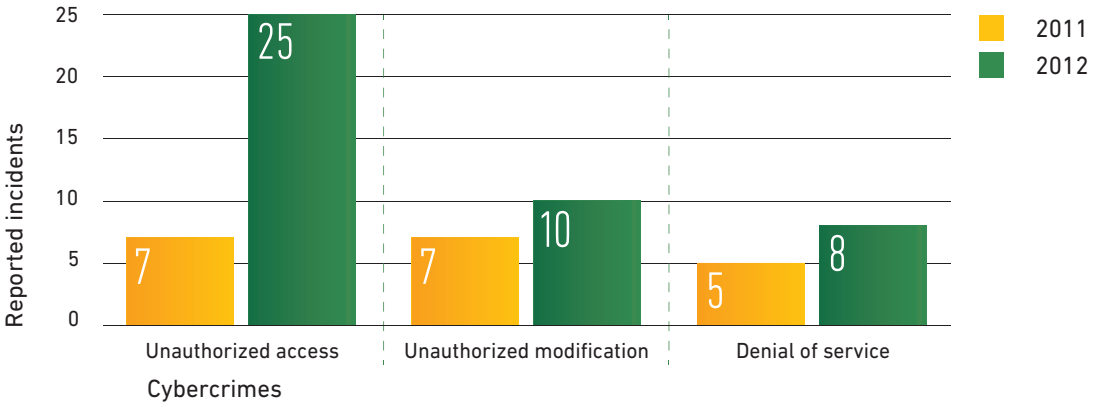



**Figure 1.** Source: Communication Forensics and Cybercrime Unit

## CYBERCRIMES FOR JANUARY - AUGUST 2014

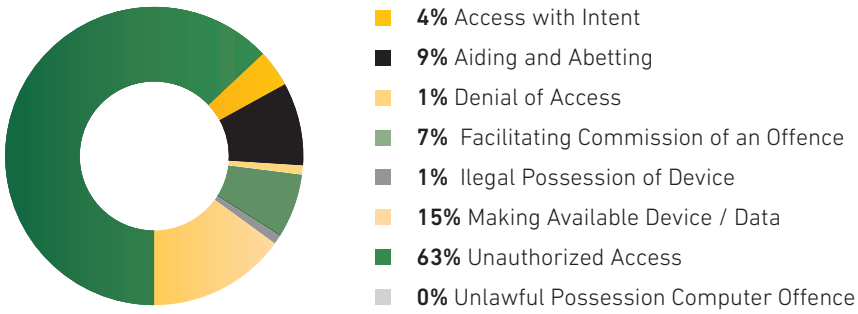
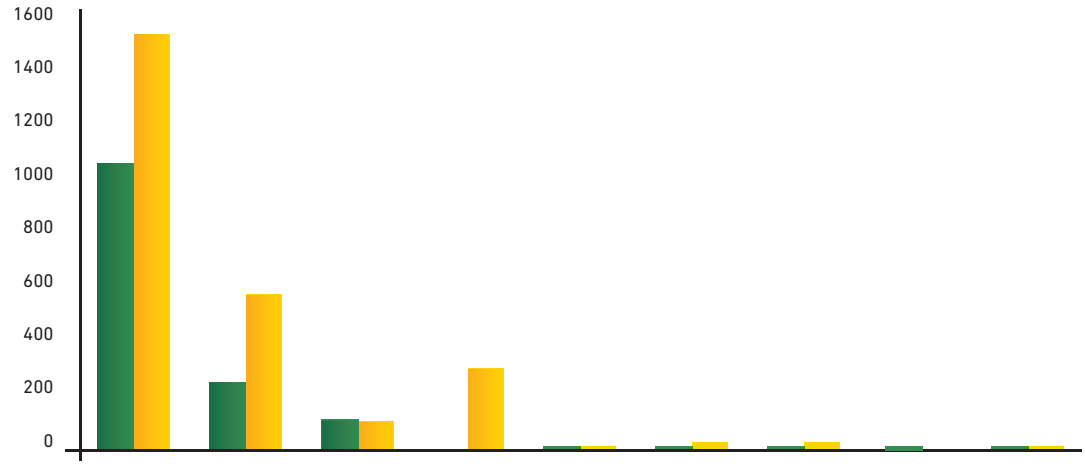



**Figure 2.** Source: Communication Forensics and Cybercrime Unit

## CYBER INCIDENTS FOR 2011 & 2012




| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **2011** | 1028 | 256 | 111 | 0 | 4 | 18 | 11 | 3 | 1 |
| **2012** | 1509 | 564 | 108 | 299 | 10 | 30 | 25 | 0 | 1 |

**Figure 2.** Source: Communication Forensics and Cybercrime Unit

CYBERCRIMES' ESTIMATED COST IS **MORE THAN THAT OF COCAINE, HEROIN AND MARIJUANA** TRAFFICKING PUT TOGETHER.

## EXISTING CYBER SECURITY RELATED EFFORTS

A lack of understanding of the mandates of the various players within this sphere can lead to stove-piped approaches resulting in conflicting legal requirements and friction between various organizations and their cyber security functions and capabilities[18]. This Strategy therefore recognizes that delineating and correlating the roles and activities of the various players is of utmost importance.

Our current reality regarding cyber security activities include:

- **Revision of the Cybercrimes Act, 2010**

Jamaica's Cybercrimes Act ('the Act') was promulgated on March 17, 2010 to address computer specific offences such as unauthorized interception, unauthorized modification of computer program or data and unauthorized access to any program or data held in a computer. The Act requires that its provisions be reviewed by a Joint Select Committee (JSC) of the Houses of Parliament after the expiration of two years from the date of its commencement[19]. An eleven member JSC was established in January 2013 to consider and report on the operation of the Act. The recommendations made by the Committee for amendments to the Act have been adopted by the Houses of Parliament and include increasing the penalties for the offences under the Act, as well as, the criminalization of actions prejudicing investigations and activities such as computer related fraud, forgery and malicious communication. Additionally, provision will be made for the forfeiture of computer material which is the subject matter of an offence in the event that the person is convicted of the said offence.

■ **Establishment of a Cyber Incident Response Team (CIRT)**
The ICT Policy, in addressing the matter of the utilization of ICT for enhanced national security, identified as a strategy, the establishment of a CIRT to address matters regarding cyber threats and appropriate responses thereto. With the assistance of the International Telecommunication Union work has commenced on the establishment of a national CIRT and the building and deployment of related technical capabilities. The CIRT will be domiciled in the Ministry with responsibility for ICT.

■ **Establishment of the National Cybersecurity Task Force**
The Government has established a National Cyber Security Task Force (NCSTF) comprising a wide cross-section of stakeholders from the public and private sector, as well as, academia. The NCSTF will, among other things,

- *formulate a strategy to develop, grow and retain high quality cyber talent for the national workforce;*
- *assist 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*
- *establish a public education and awareness programme.*

■ **Strengthening the capacity of law enforcement officers and prosecutors**
**The Communication Forensics and Cybercrime Unit (CFCU)** within the Jamaica Constabulary Force (JCF) was established in December 2010 with the merger of three (3) Units, namely the Cybercrimes Unit, Digital Forensics Unit and Communication Intelligence Unit. The CFCU which has a staff complement of 22 provides support for the investigation of all crimes.

■ **The Digital Evidence and Cybercrimes Unit** in the Office of the Director of Public Prosecution (ODPP) was established in 2009 with a view to:
*i. conducting in-depth research, preparation and prosecution of cybercrimes and cases involving digital evidence; and*
*ii. 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.*
Since its establishment the Unit has grown to twelve (12) members.

## LINKS WITH OTHER POLICIES AND PROGRAMMES

The Cyber Security Strategy will complement the following Government of Jamaica (GOJ) policies and programmes:

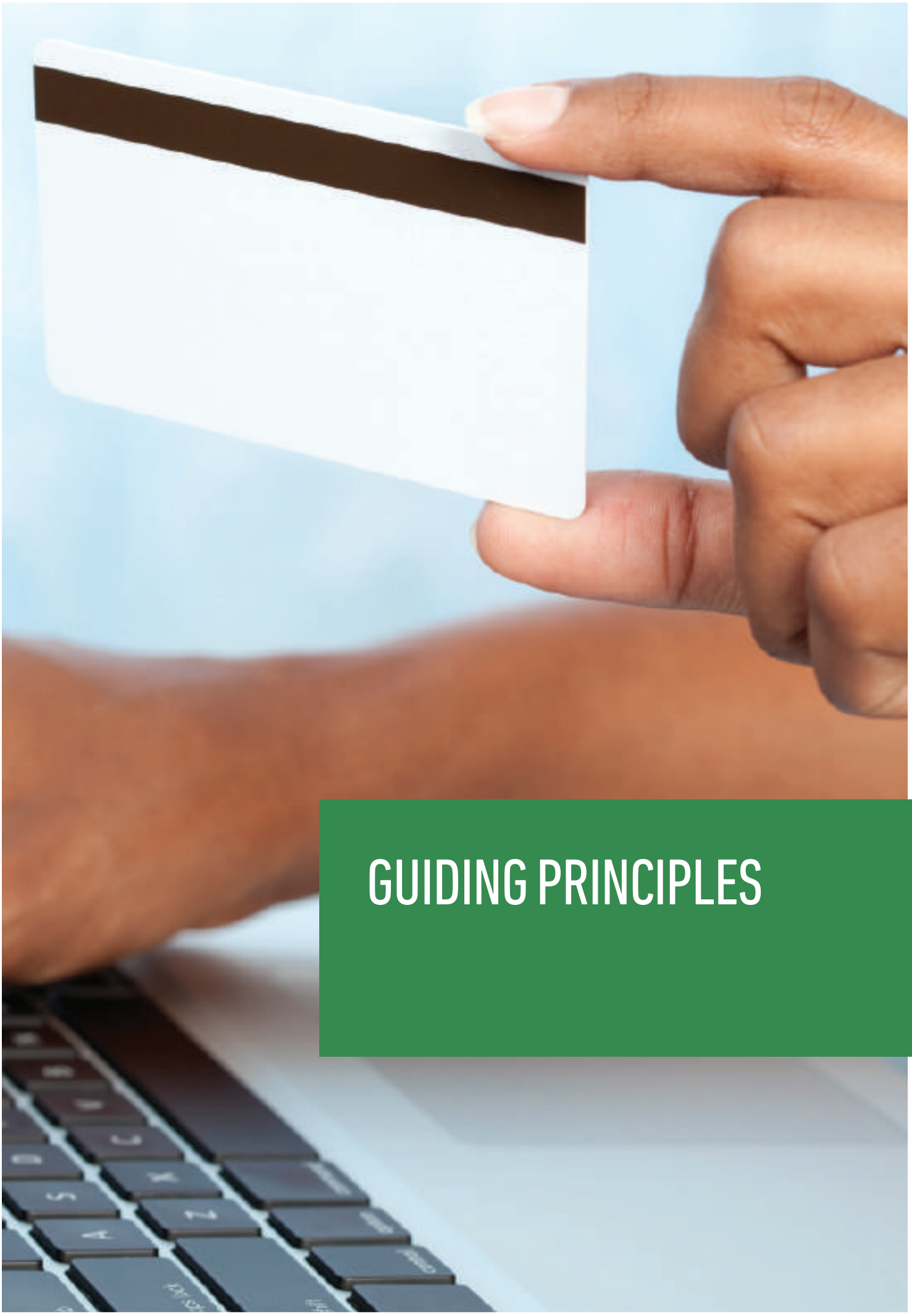
■ The National Information and Communications Technology Strategy 2007-2012;

■ The National Development Plan 2030 (Vision 2030 Jamaica);

■ The Information and Communications Technology Policy 2011; and

■ The National Security Policy 2014.

**Identity theft** is the most profitable form of cybercrime.



# GUIDING PRINCIPLES

# GUIDING PRINCIPLES

This Strategy is built on the following guiding principles:

- **Leadership:** Recognizing that the Government is responsible for policy development with respect to the ICT Sector and is one of the largest consumers of information technology services, it commits, to driving the objectives of this Strategy by adopting best practices in its operations;

- **Shared responsibilities:** All users, in enjoying the benefits of ICTs, should take reasonable steps to secure their own Information Technology (IT) systems, exercise care in the communication and storage of personal and sensitive data and respect the data and IT systems of other users. This Strategy through its development and implementation supports a multi-stakeholder approach with shared responsibility for a secure cyber framework;

- **Protection of Fundamental Rights and Freedom:** This Strategy will not impair citizens' rights under Chapter 3 of the Constitution;

- **Risk management:** In a globalized world where all internet-connected systems are potentially vulnerable and where cyber-attacks are difficult to detect, absolute cyber security is elusive. A risk-based approach to assessing, prioritizing, mitigating and resourcing cyber security activities will be applied;

- **Innovation and Business Development:** Recognizing the importance of innovation and business development to our national economy, a cyber-environment that is safe and conducive to such development will be fostered; and

- **Sustainable Resources:** A sustainable framework to ensure the availability of human capital to meet the growing and changing needs in the area of information and cyber security will be fostered.


A sustainable
framework to ensure
the availability
of human capital (...)
will be fostered

# STRATEGY OBJECTIVES

# STRATEGY OBJECTIVES

This Strategy will pursue four (4) key areas to ensure that Jamaica has a robust cyber security framework:

**NATIONAL CYBER SECURITY FRAMEWORK**


**Figure 2:** National Cyber Security Strategy objectives

## TECHNICAL MEASURES

It is important to establish an effective technical platform which includes both physical infrastructure and human capacity. The key objectives identified for this area are:

### CRITICAL INFRASTRUCTURE SYSTEMS ARE RESILIENT IN THE FACE OF CURRENT AND FUTURE CYBER THREATS

The protection of the nation's critical infrastructure is a priority and will of necessity require collaboration of all relevant stakeholders. The critical infrastructure community includes public and private entities which provide information and services which underpin the social and economic well-being of a nation. Today almost all infrastructures are becoming increasingly dependent on IT or industrial control systems (ICS) and, in many cases, both IT and ICS that guarantee their smooth and reliable operations. This Strategy will ensure that action is taken to adequately secure these systems from attacks and if penetrated there are measures in place for minimal downtime.

## NATIONAL CAPABILITY FOR ENSURING TIMELY AND EFFECTIVE RESPONSE TO CYBER INCIDENTS IS ESTABLISHED AND MAINTAINED

The timely reporting of cyber security incidents plays an important role in enhancing national cyber security. Incident reporting and analysis helps authorities to determine what should be the focus of its security measures to inform national preparedness, response and recovery efforts.

A national CIRT, with a direct reporting line to the Ministry with portfolio responsibility for ICT, will be established. The CIRT's services will include incident response, handling and coordination, vulnerability response and coordination, alerts and warnings, threat analysis, security audits and assessments, forensics and risk analysis and education and training. In its initial stages the CIRT constituents will include all government agencies and critical national infrastructure operators. Additionally, the CIRT will seek to issue timely alerts on emerging threats to ensure the integrity of systems that may be at risk, as well as, build collaborative relationships with all sectors to, among other things, foster trust.

The Strategy recognizes that cyber incidents may be as a result of criminal activities (cybercrimes) and as such interagency cooperation between the national CIRT and law enforcement will be encouraged to ensure information sharing is facilitated. A framework will be established to exchange information with its constituents regarding cyber breaches and possible counter and/or mitigation measures to be deployed.

The CIRT, given its crucial role, will adopt policies for continuous training of its staff and upgrading of its software and hardware, in order to remain current.

## A RISK BASED APPROACH IS APPLIED IN ESTABLISHING IT AND INFORMATION SECURITY STANDARDS, POLICIES AND GUIDELINES FOR ICT INFRASTRUCTURE AND CYBER SECURITY GOVERNANCE

Risk management is the process of identifying, assessing, and responding to risk and then determining an acceptable level of risk for the assets. This approach is applicable to both private and public sector assets. All relevant public and private organizations must take the necessary measures to protect their ICT infrastructure from threats, risks and vulnerabilities. As such the establishment of sector specific and general baseline security requirements will be established outlining the minimum security standards that all organizations in that sector should comply with.

The Strategy will seek to ensure that mechanisms are developed to assess existing international best practices in the area of Information Security and adapt accordingly to suit local conditions. The adoption of minimum standards for sector specific industries should result in the reduction of the number of successful attacks.

### LEVERAGING REGIONAL AND INTERNATIONAL PARTNERSHIPS

Many cyber security threats and vulnerabilities are international in nature. Cooperation with regional and international partners for purposes of information sharing as well as incident response is therefore critical.

## HUMAN RESOURCE AND CAPACITY BUILDING

In support of the vision of creating a knowledge based society, this Strategy will seek to ensure that there exists an available cadre of knowledgeable and highly skilled professionals in the area of Information Security. The key objectives identified for this area are:

### AN AVAILABLE POOL OF SKILLED AND KNOWLEDGEABLE PROFESSIONALS IN THE FIELD OF INFORMATION SECURITY IS MAINTAINED

While it is laudable that some of Jamaica's tertiary institutions offer Computer Science and/or Computing Degrees which encapsulate Information Security and Network Security programmes, more needs to be done. The challenge therefore is to increase the number and availability of professionals with a specialization in the discipline of network/cyber security. The continuously changing nature of the field requires constant training and education. The Strategy will seek to ensure that academia supports the growth and development of this field.

Sustainability in the information security ecosystem is crucial and as such accreditation and certification of skilled personnel in key positions will be pursued. A catalogue of roles, and the relevant educational background needed for key positions in Information Security will be developed. Additionally, a national register with accredited cyber-security professionals will be created and maintained.

### JAMAICA HAS AN ACTIVE AND DYNAMIC CULTURE OF RESEARCH AND DEVELOPMENT

Research and Development among stakeholders in academia, private and public sectors will be encouraged. The Government will partner with local, regional and international bodies to promote and incentivize innovation and creativity in ICT and cyber security solutions. The Strategy will seek to explore the possibility of the establishment of a fund for cyber security research and development projects.

This knowledge base will be supplemented by an exchange of information on experiences and evolving trends which will ensure not only the development of innovative products but that ICT security professionals will have timely and relevant information at their fingertips in order to perform optimally.

# LEGAL AND REGULATORY

In the context of the Government's thrust to have ICT being an enabler for all sectors, there is need to improve the legislative framework to create an environment conducive to the efficient operation of the public and private sectors and provide adequate protection for all.

## JAMAICA IS A SAFE PLACE TO DO BUSINESS

Recognizing that all businesses are affected by cyber related issues; it is the aim of this Strategy to ensure both online and offline transactions are taken into account. The legislative landscape will be periodically reviewed to ensure it is adept to treat with subject areas, such as data protection and electronic transaction and authentication and therefore support a robust business environment, while remaining compatible with international best practices.

## ESTABLISHMENT OF A ROBUST GOVERNANCE FRAMEWORK TO SUPPORT THE CYBER SECURITY LANDSCAPE

Jamaica, in this increasingly connected, global landscape must be able to effectively address threats that arise. Recognizing that all stakeholders play a role in this, a governance framework that supports a lead entity with responsibility for cyber security coordination must be established.

Experience has shown that where there are cross cutting themes between multiple agencies with similar responsibilities confusion emerges. It is imperative that the roles and responsibilities of both the private and public sector in the area of cyber security are clearly outlined. The development of a communication mechanism that delineates roles and responsibilities of key actors is crucial to the success of this Strategy.

## MAINTENANCE OF AN EFFECTIVE LEGAL FRAMEWORK AND ENFORCEMENT CAPABILITIES TO INVESTIGATE AND PROSECUTE CYBERCRIMES

It is an act in futility to implement all the measures necessary for cyber security and cybercrimes legislation if the capacities of those who are required to enforce and prosecute those laws are not taken into consideration. The JCF currently has some degree of capacity in the area of cybercrimes investigation including computer and mobile forensics. Additionally, the ODPP's Digital Evidence & Cybercrimes Unit has training in the prosecution of cybercrimes. However, there is need for greater sensitization of and/or training for other arms such as the Jamaica Defence Force, prosecutors in the Resident Magistrate Courts, as well as, the judiciary. Therefore, there will be targeted sensitization and training in cyber security and cybercrimes for these stakeholders.

The legislative framework should support regional and international collaboration for example, investigations across borders and successful prosecution of trans-border crimes. Additionally, consideration will be given to being party to international conventions and mechanisms that support Jamaica's vision and is in line with the Constitution.

### LEGAL PROTECTION IN CYBERSPACE

There will be dedicated efforts to ensure that the legislative framework for cybercrime adequately addresses emerging threats and trends while preserving the right to privacy and other fundamental rights and freedoms. There will be no discrimination in the application of the law; as once a person falls victim to a cybercrime within the jurisdiction there will be legal recourse.

## PUBLIC EDUCATION AND AWARENESS

Increasing awareness about cyber-security threats and vulnerabilities and their impact on society has become vital. While there has been increased adoption of ICT solutions in everyday life, there has not been the same level of appreciation of the associated risks involved. Through public education and awareness programmes individuals and corporate users can be informed of appropriate online behaviour and thus better protect themselves.

### JAMAICANS ARE KNOWLEDGEABLE AND AWARE OF THE CYBER RISKS, AS WELL AS, THE ACTIONS TO BE TAKEN REGARDING CYBER SECURITY

It is a priority that all Jamaicans should feel confident while using various online platforms. As the Internet becomes more accessible through various devices such as tablets, mobile phones, game consoles, and with the advent of the IoT, more personal and financial information will be exposed online. In this unregulated space of the Internet, mechanisms must be implemented to educate users on the risks and the steps that can be taken to mitigate their chances of becoming a victim, as well as, equip them with the necessary tools to protect themselves.

Therefore, the national level of awareness about cyber security and the risks inherent in the use of the Internet will be assessed and appropriately tailored sensitization programmes developed to inform the Jamaican population.

### MEASURES ARE IMPLEMENTED TO PROTECT VULNERABLE GROUPS IN CYBERSPACE

It is the Government's responsibility to establish measures which protect the vulnerable in our society, such as, the elderly, youth and persons with disabilities, as they often lack the wherewithal to do so themselves. As the guardian of their interests it is the Government's responsibility to ensure that they are not overlooked but are informed and aware of the risks. Programmes that will encourage the adoption of safe online practices will be developed and the assistance of service providers will be sought to provide built in tools to protect this group where possible.

### JAMAICA HAS A CULTURE OF CYBER SECURITY

While, it is important to empower Jamaicans with the information and practical tools needed to protect themselves online. It is equally, important for individuals to take the security of their own personal data seriously and


practice good habits while navigating the Internet, downloading applications or sharing information for both business and personal reasons.

In a similar vein businesses will have to implement measures to ensure the protection not only of their data but that of their customers. This should extend to employee security awareness and training programs especially with the wide adoption of bring your own device (BYOD) policies. Employee awareness is critical to the success of any security program. It has been noted that adversaries often target employees using social engineering schemes and thus businesses should implement effective employee training programmes to ensure the integrity of their systems is not compromised.

The Strategy will seek to improve the level of awareness of information security, monitor and develop information skillsets though a proactive plan for communications for all sectors of society. Additionally, businesses will be encouraged to adopt self-regulation in the various sectors to ensure the security not only of their data but that of their customers.

# IMPLEMENTATION AND REVIEW

# IMPLEMENTATION AND REVIEW

The implementation of the Strategy will be led by the Ministry with responsibility for ICT. A detailed outline of the activities associated with the aforementioned strategic objectives is annexed. It is intended that the Ministry with responsibility for ICT and the NCSTF will develop an Implementation Plan to carry out the objectives and activities outlined in this Strategy within three (3) months of its adoption. This will involve the delineation of specific tasks associated with the objectives and activities identified and the allocation of responsibilities to specific entities for execution. It is envisioned that the preparation of the Implementation Plan will go hand in hand with a review of this Strategy, which will be revised and updated every three (3) years or as necessary.

# CONCLUSION

# CONCLUSION

As Jamaica embraces the benefits of ICT for socio-economic development and seeks to position itself as a regional leader it must adopt and implement best practices in cyber security in all facets of its economic and social life. Recognising this inextricable interplay between socio-economic development goals and national security strategies, this Strategy will play an implicit and explicit role in securing the networks needed to support the realisation of the nation's development goals (Figure 3). Tackling the issue of cyber security from this holistic approach therefore will ultimately impact Jamaica's vision of having a stable and prosperous economy.

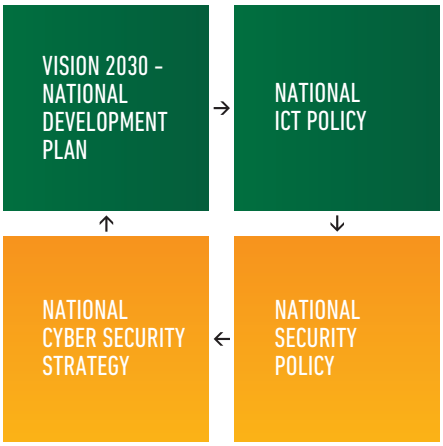



**Figure 3.** Interplay between national strategies and cyber security

Decisively, this Strategy, following the outlined guiding principles, seeks to prepare Jamaica for existing and emerging cyber threats and risks by:

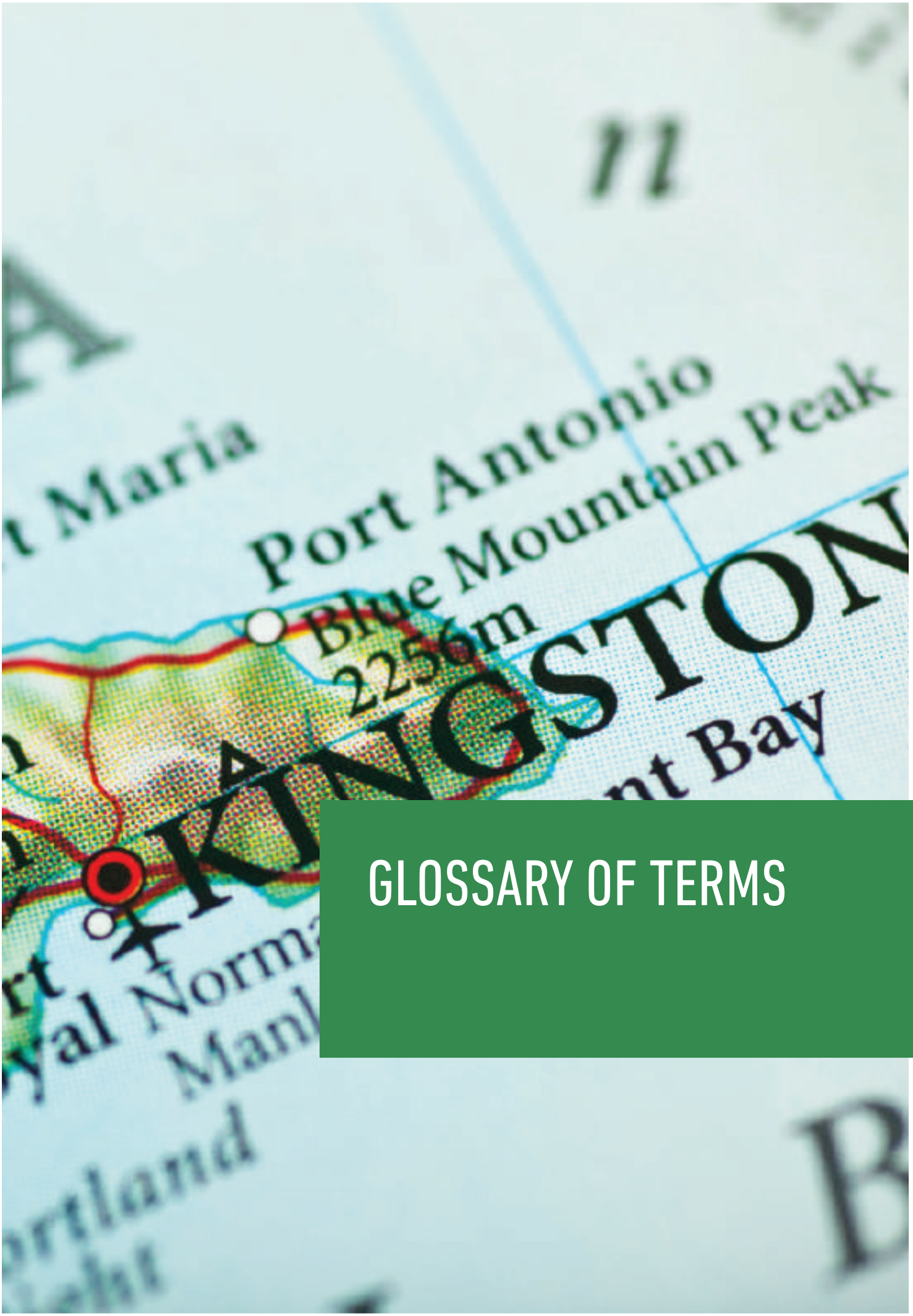
1. Promoting a secure and reliable environment for businesses to develop efficient and innovative business solutions;

2. Promoting the development of innovative and cutting-edge solutions through the implementation of research and development programmes in cyber security;

3. Developing and maintaining efficient capabilities to prevent, detect, respond and recover from, malicious attacks while implementing measures to provide adequate protection for critical infrastructure as well as the vulnerable in our society;

4. Ensuring that the quality of education and training meets the developmental needs of the country in a dynamic discipline; and

5. Providing an enabling legal framework that promotes the utilization of ICT while penalizing perpetrators when they are caught.




# GLOSSARY OF TERMS

# GLOSSARY OF TERMS

In this document, where the context allows, the following terms will have the meanings specified below:

Botnet - is a group of Internet-connected personal computers that have been infected by a malicious application (malware) that allows a hacker to remotely control the infected computers or mobile devices without the knowledge of the device owners.

Critical Infrastructure - include systems and assets, whether physical or virtual, so critical that the incapacitation or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. This may include water and sewage networks, agriculture, health systems, emergency services, information technology and telecommunications, banking and finance, energy (electrical and wind generated), transportation (air, road, port), postal and shipping entities.

Cybercrime – is a crime in which a computer is the object of the crime or is used as a tool to commit an offence.

Cyber security - is the implementation of measures to protect ICT infrastructure including critical infrastructure from intrusion, unauthorized access and includes the adoption of policies, protocols and good practices to better govern the use of cyberspace.

Cyber Incident Response Team (CIRT) - is a team of dedicated information security specialists that prepares for and responds to cyber security breaches.

Denial of Service – is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet usually by flooding the target resource with external communication requests.

Information Security - is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are understood for these purposes as being interchangeable.

National Cyber Security Task Force (NCSTF) - established in June 2013 to create a framework to facilitate the building and enhancement of confidence in the use of cyberspace and protection and security of related assets the through collaboration amongst all the stakeholders; with view

to advancing Jamaica's economic and social interests and maintaining national security under all conditions.

Phishing - is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Self-regulation - is the process whereby an organization is asked, or volunteers, to monitor its own adherence to legal, ethical, or safety standards, rather than have an outside, independent agency such as a governmental entity monitor and enforce those standards.

Stove-piped – is a structure which largely or entirely restricts the flow of information within the organisation to up-down through lines of control, inhibiting or preventing cross- organisational communication.

Unauthorized Access – is to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network without authorization.

Unauthorized Modification –is the unlawful alteration, erasure or addition of any program or data to the contents of a computer or computer systems.

# ACTIVITIES

# ANNEX

## Activities

Key for Timeline:
Long Term - within 3 years
Medium Term - within 2 years
Short Term - within 1 year

## TECHNICAL MEASURES

| Objectives | Activities | Timeline | Lead Role |
|---|---|---|---|
| **Critical infrastructure systems are resilient in the face of current and future cyber threats** | 1. Create a robust national response and recovery capability for IT systems critical infrastructure systems.<br>2. Ensure that measures are in place to guarantee continuity of operations of all critical infrastructures after a system compromise.<br>3. Promote and encourage adherence to international best practices among owners and operators of critical infrastructure.<br>4. Encourage self-regulation by the owners and operators of critical infrastructure.<br>5. Develop a system of reporting by owners and operators of critical infrastructure to the Government of any major security breaches detected. | Medium Term | MSTEM, eGov Jamaica Ltd and owners and operators of Critical Infrastructure |
| **National capability for ensuring timely and effective response to cyber incidents is established and maintained** | 1. Establishment of the CIRT with operational and administrative procedures inclusive of continuous monitoring of the national infrastructure and networks to ensure continuity and development.<br>2. Establish fraternal links to international CIRTs with protocols for engagement.<br>3. Conduct continuous risk assessment to determine current and future threats, as well as, develop and maintain a threat list.<br>4. Issue early warnings to stakeholders on a continuous basis to reduce exposure to risks. | Short –Medium Term | MSTEM, CIRT |

| Objectives | Activities | Timeline | Lead Role |
|---|---|---|---|
| | 5. Provide future threats analysis to critical stakeholders and provide information to decision makers to guide the allocation of key assets.<br>6. Establish a line of communication between the CIRT and law enforcement when cyber incidents are detected for their investigation and conversely to the CIRT whenever a threat is detected by law enforcement.<br>7. Development of contingency planning methodologies for various sectors especially for critical and essential services.<br>8. Conduct cyber incident response exercises. | | |
| **A risk based approach is applied in establishing IT and information security standards, policies and guidelines for ICT infrastructure and cyber security governance** | 1. Assess and research existing IT and Information Security standards for the protection ICT infrastructure.<br>2. Conduct a national vulnerability assessment and develop and publish standards and guidelines based on the results of the assessment.<br>3. Implement Government wide IT and Information Security standards, policies and guidelines and monitor and enforce their implementation.<br>4. Encourage the adoption and implementation of stipulated IT and Information security standards, policies and guidelines by all individuals and institutions. | Medium-Long Term | MSTEM, CIRT, Private Sector |
| **Leveraging regional and international partnerships** | 1. Conduct a stakeholder mapping exercise and develop a strategic outreach programme for the engagement of regional and international partners.<br>2. Utilize regional and international cooperation to improve the technical capacity of cyber security professionals within the government and private sector to enhance the capability to respond to cyber threats.<br>3. Establish mechanisms for secure information sharing with regional and international stakeholders.<br>4. Pursue areas of collaboration with other CIRTs (regionally and internationally). | Medium Term | MSTEM, MNS, ODPP, MFAFT, MOJ, CIRT |

# HUMAN RESOURCE AND CAPACITY BUILDING

| Objectives | Activities | Timeline | Lead Role |
|---|---|---|---|
| **An available pool of skilled and knowledgeable professionals in the field of Information Security is maintained** | 1. Conduct on an ongoing basis an assessment of the existing and available pool of human resource in the area of Information Security.<br>2. Modify school curricula for secondary and tertiary students to expose and bring focus to information security.<br>3. Specify minimum professional and academic standards for entry into employment in the field of information security.<br>4. Establish targeted training in cyber security for specific stakeholders such as MSMEs, members of the public sector, judiciary, law enforcement and military.<br>5. Actively engage in talent recruitment initiatives in the cyber security field.<br>6. Promote careers in Information Security.<br>7. Promote the adoption by all stakeholders of human resource training policies that will ensure continuity of cyber security operations and implementation of best practices.<br>8. Collaborate and facilitate exchanges with other institutions with capability and knowledge in cyber security. | Medium Term | MSTEM, MOE, CIRT, MOJ, MNS, OPM, MOFP, Educational Institutions, Private Sector |
| **Jamaica has an active and dynamic culture of research and development** | 1. Foster the development of cyber security products and services through research and development.<br>2. Develop joint research and development projects between public and private sectors and academia (nationally, regionally and internationally) to build innovative cyber security solutions.<br>3. Develop a forum to facilitate the exchange of knowledge among stakeholders. | Short- Medium Term | MSTEM, CIRT , Private Sector and Multilateral and Bilateral donors |

| Objectives | Activities | Timeline | Lead Role |
|---|---|---|---|
| | 4. Identify and access available resources (national, regional and international) that provide capacity building for cyber security.<br><br>5. Explore the opportunities for the establishment of a fund dedicated to capacity building in cyber security through public private partnership.<br><br>6. Promote scholarship programmes or funding for the development of cyber security innovations. | | |

## LEGAL AND REGULATORY

| Objectives | Activities | Timeline | Lead Role |
|---|---|---|---|
| **Jamaica is a safe place to do business** | 1. Assess the legislative framework that supports cyber security issues with a view of identifying gaps and recommend measures to fill these gaps.<br><br>2. Establish a continuous review process to ensure that there is an updated and robust legislative framework that is appropriately aligned with international best practice and creates a safe environment for all activities within the cyber domain including:<br>**a.** Data Protection<br>**b.** Cybercrimes<br>**c.** Privacy<br>**d.** Electronic Transaction including authentication<br>**e.** Electronic/digital evidence<br>**f.** Intellectual Property | Short-Medium Term | MSTEM, MOJ, MNS |
| **Establishment of a robust Governance framework to support cyber security landscape** | 1. Define and ensure that there is a proper governance framework for cybersecurity.<br><br>2. Create an environment that supports the exchange of information in the area of cyber security both nationally and internationally. | Medium – Long Term | MSTEM, MOJ, MNS, JCF ODPP, Private Sector |

| Objectives | Activities | Timeline | Lead Role |
|---|---|---|---|
| **Maintenance of an effective legal framework and enforcement capabilities to investigate and prosecute cybercrimes** | 1. Broaden and improve the capabilities of the bodies responsible for investigating and prosecuting cybercrimes (including judiciary, law enforcement and prosecutors).<br>2. Promote the exchange of information, intelligence and expertise with respect to cybercrimes and encourage cooperation with national, regional and international entities.<br>3. Ensure that legal and law enforcement professionals have access to training that provides them with the necessary level of knowledge to apply the associated legal and technical framework more effectively.<br>4. Enhance cyber security awareness among legal and law enforcement professionals about the trends in cyber security and cybercrime. | Medium – Long term | MSTEM, MOJ, MNS, JCF ODPP, Civil Society |
| **Legal protection in cyberspace** | 1. Pursue cyber security policies and legislation that preserves the right to privacy and other fundamentals rights and freedoms.<br>2. Review legislative landscape to ensure adequate protection of vulnerable groups within the society, such as children, disabled, elderly, from cyber threats.<br>3. Actively pursue bilateral and multilateral agreements to support law enforcement activities in cross border attacks against Jamaican citizens. | Short-Medium Term | MSTEM, MOJ, MFAFT, MNS |

# PUBLIC EDUCATION AND AWARENESS

| Objectives | Activities | Timeline | Lead Role |
|---|---|---|---|
| **Jamaicans are knowledgeable and aware of cyber risks, as well as, the actions to be taken regarding cyber security** | 1. Conduct a national assessment on the level of awareness and explore the various marketing strategies to inform the public awareness campaign.<br>2. Launch Public Awareness campaign targeted at specific groups and the general public.<br>3. Develop public private partnerships and collaborative relationships to build awareness in cyber security. | Short Term | MSTEM, JIS, MNS, CIRT, Private Sector |
| **Measures are implemented to protect vulnerable groups in cyberspace** | 1. Implement programmes that promote the adoption of safe practices online by vulnerable groups within the society including children, women, aged, mentally challenged and returning residents.<br>2. Encourage stakeholders to incorporate protective tools and measures, targeted at protecting the vulnerable groups, into the products and services offered. | Medium- Long Term<br>Ongoing | MSTEM, MLSS, MYC, MOH Civil Society Groups and Private Sector |
| **Jamaica has a culture of cyber security** | 1. Establish a National Cyber Security Day, working in tandem with other initiatives such as Internet Day, with the aim of raising and promoting awareness in the key areas of cyber security.<br>2. Identify and leverage, through Private and Public Partnerships at the national, regional and international levels, existing resources for increasing cyber security awareness.<br>3. Ensure that current and applicable information related to cyber security is easily accessible to the Jamaican population.<br>4. Establish policies and guidelines across the public sector to engrain cyber security awareness and best practices in the implementation of all relevant initiatives and projects. | Long Term | MSTEM, MNS, CIRT, JIS Private Sector |