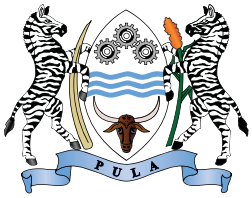

Republic of Botswana
Ministry of Transport and Communications

National Cybersecurity Strategy

MISSION STATEMENT

Exist to protect information infrastructure, provide information security assurance, build capacity and capabilities to prevent and respond to cyber threats in order to enhance the socio-economic development of Botswana

TABLE OF CONTENT

ACRONYMS....3
FOREWORD....5
EXECUTIVE SUMMARY....7
1.0 INTRODUCTION....8
1.1 Background....8
1.2 Situational Analysis....9
1.3 Policy, Legal and Regulatory Framework....11
1.4 Rationale....11
2.0 CONTEXT – SOCIO-ECONOMIC, RISKS AND THREATS....13
2.1 Society....13
2.2 Electronic Commerce (e-Commerce)....13
2.3 e- Government Services....13
2.4 Risks and Threats....14
3.0 STRATEGIC FOUNDATIONS....15
3.1 Vision & Mission Statement....15
3.2 Core Values....15
3.3 Strategic Objectives....17
3.4 Strategic Objectives and Initiatives....18
4.0 IMPLEMENTATION....28
4.1 Critical Success Factors....28
4.2 Governance Framework....29
4.3 Roles and Responsibilities....30
4.4 Funding Resources....36
4.5 Monitoring and Evaluation....36
GLOSSARY....38

ACRONYMS

BIDPA - Botswana Institute for Development Policy Analysis

BOCRA- Botswana Communications Regulatory Authority

CERT - Computer Emergency Response Team

CII - Critical Information Infrastructure

CNI - Critical National Infrastructure

CIRT - Computer Incidents Response Team

CTO - Commonwealth Telecommunications Organisation

GoB - Government of Botswana

HRDC - Human Resource Development Council

ICT - Information and Communications Technology

IIS - Important Information Systems

IPV4 - Internet Protocol Version 4

IPV6 - Internet Protocol Version 6

ISP - Internet Service Provider

IT - Information Technology

M&E - Monitoring and Evaluation

Maitlamo Policy -Botswana's National Information and Communications Technology

MDJS - Ministry of Defence, Justice and Security

MFEP - Ministry of Finance and Economic Development

MIH - Ministry of Infrastructure and Housing Development

MLGRD - Ministry of Local Government and Rural Development

MOPAGPA - Ministry of Presidential Affairs, Governance and Public Administration

MNIG - Ministry of Nationality, Immigration and Gender Affairs

MMGE - Ministry of Mineral Resources, Green Technology and Energy Security,

MoBE - Ministry of Basic Education

MoTE - Ministry of Tertiary Education, Research, Science and Technology

MIAC - Ministry of International Affairs and Cooperation

MOHW -Ministry of Health and Welness

MTC - Ministry of Transport and Communications

MITI - Ministry of Investment, Trade and Industry

MYSC - Ministry of Youth Empowerment, Sport and Culture Development

MELSD - Ministry of Employment, Labour Productivity and Skills Development

NBS - National Broadband Strategy

NCAC - National Cybersecurity Advisory Council

NCII - National Critical Information Infrastructure

NCOC - National Cybersecurity Operation Centre

NCTRC -National Cybersecurity Training & Research Centre

NDFL - National Digital Forensics Lab

OP - Office of the President

PKI - Public Key Infrastructure

FOREWORD

Information and Communications Technologies (ICTs) have transformed the lives of Batswana. They have had positive impact on the economy, enabling its growth and efficiencies on service delivery. Through the envisaged National Broadband Strategy (NBS), the Government of Botswana would like to further enhance the role of ICT, particularly cyberspace in socio-economic and political aspects of the country. However, the Government is conscious of the risks, threats and vulnerabilities to the citizens and the country posed by misuse of cyberspace. It is for this reason that the Government, working in concert with the private sector, developed a National Cybersecurity Strategy to provide a framework for a secure cyberspace in Botswana. The Strategy is aimed at the public, to raise awareness and build capacity among them to safeguard against cyber threats, for the industry and Government to always be prepared to prevent, defend and act against any cyber-attacks.

The development of the National Cybersecurity Strategy (NCS) will enable the Government of Botswana and other stakeholders, to establish appropriate measures that will ensure Confidentiality, Integrity and Availability (CIA) of networks, systems and data of the information communicated, processed and stored through electronic or equivalent means. Because cyber-attacks are not limited by national boundaries, passing through multiple networks in different countries, it is important to engage with all relevant stakeholders in developing the National Cybersecurity Strategy. It is essential that cyber security requirements are "bake it in" in initial design and development of the ICT systems rather than to be "bolted on" at the later stage of the development cycle.

The development of the National Cybersecurity Strategy was led by the Ministry of Transport and Communications and it included all the relevant stakeholders from the Private Sector, relevant Ministries, Regulator, and Academia. The Commonwealth Telecommunications Organisation (CTO) assisted with the development of the National Cyber Security Strategy with funding from the United Kingdom of Great Britain Government's Foreign & Commonwealth Office (FCO). The United Kingdom of Great Britain further contributed by providing comments on the draft strategy. In addition, the project team which developed National Cyber Security Strategy benefited from inputs and comments from the United States of America (USA) State Department, through the technical consultant from MITRE and Carnegie Melon University. On behalf of the Government of Botswana. I would like to thank all who assisted with the development this strategy.

The main aim of the National Cybersecurity Strategy is to have a high-level top down approach cyber security framework that clearly establishes national objectives, sets priorities, specifies timeframes and outlines the roles of the various stakeholders. Cyber threats by their nature do not discriminate between big and small institutions

and individuals; there are many examples of cyber incidents against multi-national corporations and individuals. Cyber threats can be complex. Therefore, ordinary individuals with less sophistication and means may require to be continuously assisted and educated, to keep up with evolving threats. These threats and risks are ever presents. Therefore, it is very important that Government and other key stakholders, play an active role in addressing the National Cybersecurity Strategy.

To ensure effective implementation of the National Cybersecurity Strategy, an implementation plan with clear key performance indicators has been developed to monitor and validate that the objectives of the strategy are achieved. The appropriate mechanisms and framework will be put in place to ensure that the key performance indicators and desired outcomes are realised.

As the Ministry responsible for ICT, we believe that the National Cyber Security Strategy will provide appropriate guidance in addressing the issues of Cyber Security which require a multi-stakeholder approach.

.....

Honourable Minister Onkokame Kitso Mokaila

MINISTER OF TRANSPORT AND COMMUNICATIONS

EXECUTIVE SUMMARY

Information and Communications Technology (ICT), is increasingly transforming societies and enabling the growth of the global economy. The adoption of ICT within a country's economy provides enormous benefits through improved efficiencies and effectiveness in service delivery, cost savings, improved productivity, transparency as well as accountability. Digital infrastructures are emerging as the backbone of a successful economy, a vibrant research community, a transparent state as well as a free society.

Botswana is gradually leveraging ICTs in its critical areas such as communications, governance, utility provision, healthcare, financial and transport sectors. This has led to the emergence of possible threats and risks against the National Critical Information Infrastructure. The risks and threats must be mitigated against. Cybersecurity is now taking centre stage in ensuring that critical infrastructure is protected through continuous risk assessment, putting in place appropriate mitigations, creating appropriate collaborations, having in place relevant and effective cyber security capabilities, accompanied by cybersecuritry awareness. It's for this purpose that Botswana developed a National Cybersecurity Strategy. The strategy addresses the current challenges within Botswana and proposes strategic action areas to improve our cybersecurity maturity.

The objective of this strategy is to create a cohesive and inclusive approach to delivering a safe, secure and resilient cyberspace and a comprehensive framework to facilitate coordinated responses by Government, the private sector, and other partners to address issues of cyber security.

The National Cybersecurity strategy is organised as follows: - Introduction section provides the background information, situational analysis in relation to the Cybersecurity and also provides the rationale and justification for the development of a National Cybersecurity Strategy. Section 2 contextualises issues of Cybersecurity in relation to Botswana in terms of the benefits, risks and threats arise in the cyberspace. The strategic goals and objectives are discussed in section three and the final section discusses the implementation, roles and responsibility, monitoring and evaluation issues.

1.0 INTRODUCTION

1.1 Background

The National Cybersecurity Strategy sets out how Botswana intends to create a resilient, safe and secure ICT operational environment. The strategy is aimed towards the members of the public, industry, international partners and the Government. The strategy aims to provide awareness to members of the public on threats, risks in the cyberspace and interventions. For the Government and Industry, it's a call to arms, for them to take action and provide necessary resources. The strategy also lays out its principles, which will help Botswana to collaborate and cooperate with interested international partners with similar values.

The rapid proliferation and adoption of ICT services and infrastructure in Botswana is transforming how citizens, the private sector, and the Government interact, inform themselves, participate and contribute to the well-functioning of society. However, this has also resulted in the introduction of new types of risks, in the form of cyber threats or attacks. These threats affect service provision and trust in the use of ICT. The increase in cybercrime sophistication and occurrence requires a proactive approach to ensure that risks are continually assessed and mitigations put in place. While most Batswana have taken up technology, there has not been a corresponding rise in public education and awareness on cyber security issues.

Cybersecurity has been identified as a critical issue in Botswana. The National Development Plan 11 covering the years 2017-2023, states that cyberspace threats and risks should be dealt with during the NDP implementation. The NDP 11 further notes that since cybersecurity threats are imminent and worrisome, it is appropriate for legislation to combat cybersecurity to be developed during NDP 11. Under NDP 11 headings of *ICT* and *Secure Cyber Space,* secure cyber space is identified as one of the factors that would support the economy, in particular key priority areas of water, agriculture, power, tourism and job creation.

Botswana has done relatively well in providing formal education to its population and provision of necessary infrastructure that facilitates communications and service delivery through Information and Communication Technologies. The country, however, has limited capacity on Cyber Security expertise. The issues of Cyber Security require a multi-stakeholder approach due to the diverse nature of the cyberspace. Currently, in Botswana there is no coordinated framework for addressing the cyber security issues among the various stakeholders. One of the objectives of this strategy is to clarify the roles of the various key stakeholders, both public and private, in addressing the country's cybersecurity challenges.

ICT sector or cyberspace depends on Critical Information Infrastructure (CII) that can be accessed via internet or otherwise, and also goes beyond territorial boundaries. This makes protecting this infrastructure more complex, given that it also brings in third parties in the form of other countries. It is for this reason that

international cooperation and collaboration plays a central role in the National Cybersecurity Strategy (NCS). An open and free internet, the protection of personal data as well as the integrity of interconnected networks are critical for overall prosperity, security and the promotion of human rights in Botswana. This strategy provides a multi-stakeholder framework for ensuring the safety, security and reliability of Botswana's cyberspace.

1.2 Situational Analysis

In 2012 the country carried out cyber security assessment assisted by the International Telecommunication Union (ITU) and International Multilateral Partnership Against Cyber Threats (IMPACT) to assess the country's readiness for establishing a National Computer Incident Response Team (CIRT), which will assist in responding to the cyber security threats[1]. The study found that Botswana has a well-developed ICT infrastructure with fibre-optic cables linking the major population centres. In addition the country has international connectivity through WACS, SEACOM and EASSY undersea cables. The community is well connected with mobile network covering more than 90% of the population. Internet usage is increasing throughout the country with many people using the mobile services to access the Internet, more especially the social media; the country's mobile broadband subscription was 1 409,274 as of Dec 2016**.**

1.2.1 Summary of the Key Findings of the Assessment

i) Cyber security is not allocated sufficient priority in policy making and on the on-going ICT projects. Also, Cyber security principles are not adopted by government in all the projects related to ICT.

ii) Critical National Information Infrastructure (CNII) has not been identified and there is no defined cyber security strategy in place to manage and mitigate cyber security incidents in case of a coordinated cyber-attack on the critical national information infrastructure. It was recommended that the Country should develop a National Cyber Security Strategy that will clearly define roles of the various stakeholders and develop measures and procedures for the protection of CNII

iii) Appropriate legislation, policies and regulations on cyber security are inadequate to address the current cyber security challenges.

iv) Training, specifically in the area of cyber security needs to be improved; all stakeholders such as regulators, Law Enforcement Agencies, Judiciary, Prosecutors, Service providers, Financial Institutions, service providers need to have adequate capacity and capability to handle matters related to cyber security.

[1] The Full report of ITU/Impact CIRT Readiness assessment Report can be assessed at www.bocra.org.bw

v) There is no proper coordination or mechanism dealing with monitoring, detection, tracking and mitigation of cyber-attacks and cyber threats at national level . There is no coordination on cyber security issues public awareness. It was recommended that the country should establish a National Computer Emergency Response to monitor and detect cyber threats, as well as educate the public.

vi) The report noted that the country has had reported cases of some cybercrime activities and threats such as Money laundering, online Scams, Hacking, Malwares, Viruses and worms, Identity Theft, Frauds, SPAM etc. Most of these were addressed on ad hoc basis by various institutions

vii) The study recommended that the country should develop and implement awareness campaigns to educate users, law enforcement officers and policy makers about cyber laws, the impact of cybercrime and measures of combating it.

1.3 Policy, Legal and Regulatory Framework

Botswana has developed a number of policies, regulatory and legislative instruments which currently provide direction and guidelines on cybersecurity. The country has no data protection and privacy law. Neither does it have any national governance roadmap for cybersecurity. Some of the legislations and policies currently in place that address cybersecurity related issues are:

- ***Cybercrime and Computer Related Crimes Act*** No. 22 of 2007 which is intended to: combat cybercrime and computer related crimes, repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence. The Act is currently being reviewed to address the latest technology changes and related cybercrimes.

- ***Communications Regulatory Authority Act*** No. 19 of 2012, which provides for the regulation of the communication sector, comprising telecommunications, Internet, Radio communications, Broadcasting, Postal services and related matters.

- ***Electronic Communications and Transactions Act*** No. 14 of 2014 is intended to provide for the facilitation and regulation of electronic communications and transactions. It is to provide specifically for electronic commerce and electronic signatures as well as for matters incidental and connected thereto. The associated secondary legislation (regulations) have also been developed.

- ***"Electronic Records (Evidence) Act*** No. 13 of 2014***.*** The Act provides for the admissibility of electronic evidence in legal proceedings and authentication of electronic evidence. The associated secondary legislation (regulations) have also been developed.

- The National Information and Communications Technology Policy commonly called ***(Maitlamo)"*** has also been adopted by the Country to guide the development of ICT throughout the country.

1.4 Rationale

Cyber security is a global challenge. Thus, a co-ordinated multi-sector response provides a route to building public confidence and trust in the use of ICTs. These efforts rely on national actions among countries of the world, Botswana included.

One of the key challenges that the Government of Botswana is facing in this information age is to ensure that the nation is secure against cyber threats. Botswana is experiencing a growing dependence on Cyberspace for the delivery of services essential to people's daily lives, commerce, National security, innovation and the general free flow of information. The increasing dependency on ICTs by both public and private sectors, makes protection and sharing of information more critical in order to protect the economic interests and security of Botswana and her citizens.

A number of new and major risks exist in cyberspace such as: organised crime in cyberspace, hacktivism, cyberattacks, unplanned disruptions to network integrity and security due to human errors or factors, cyber terrorism, abuse of personal data, child online pornography, loss of money or data due to activities in cyberspace, etc. With the increase in sophistication of these cyber threats, risks, and cybercrime over the years, the necessity of developing a coherent approach to effectively detect, prevent and mitigate both current and future Cyber threats arises, hence the motivation to develop a National Cybersecurity Strategy for Botswana.

The strategy will help initiate a systematic national programme to defend cyberspace from threats irrespective of their origin. Critically, the strategy prioritises cyber threats and risks as well as allocation of responsibilities, to ensure that all relevant stakeholders accept responsibility for and take appropriate steps to enhance cybersecurity. As a result, the strategy aims to improve security by creating stakeholders awareness on relevant risks, preventive measures and effective responses.

2.0 CONTEXT – SOCIO-ECONOMIC, RISKS AND THREATS

2.1 Society

Cyberspace has developed into a vital area of activity for the state, the economy, science and society in general. Everything in the information age is connected to the Internet and everything is connected to each other. This promotes innovation and enhances productivity. It is estimated that there will be 50 billion devices connected to the Internet by 2020 enabling them to communicate with each other (compared to 15 billion today)[2]. By the end of 2015, there were more than 3.2 billion Internet users globally, with a sizeable population of Batswana amongst them.

Cybersecurity is an ecosystem that goes beyond the use of technology. It includes non-technical measures such as delivery of timely and appropriate policy and regulatory responses, capacity building and consumer awareness. The main objective of the National Cybersecurity Strategy is to ensure that Citizens have access to an open cyberspace with confidence that their data will be protected.

Batswana use social media for advocacy on socioeconomic and political issues. It is also a platform reach out to target audience instantaneously, at a fraction of the cost of traditional media advertising. Examples include entertainment industry reaching out to audience beyond border and government delivering the public services (e-gov services) through the online platforms. Therefore, it is important to ensure that cyberspace is secure to guarantee public confidence and integrity on the Internet.

2.2 Electronic Commerce (e-Commerce)

Cyberspace has developed into a market place of strategic importance in a relatively short period of time. The country has enacted the Electronic Communications and Transactions Act in order to facilitate e-commerce and is in the process of developing an e-commerce strategy. Some businesses are already trading online and also use the Internet to market their products on the global market. While Botswana's participation in online market is still at its infancy stage, it is expected to grow once the country has developed and implemented an e-Commerce strategy. It is important for Botswana to be part of the digital economy, using e-commerce to drive the economic diversification.

2.3 e- Government Services

The Internet plays an important role in facilitating the communication between Government and society. The Government has developed an e-government strategy to provide online services. Cyberspace has an impact on the relationship between the Government and society. The Government portal is already online. Social media

[2] *Source: A collaborative report by DHL and Cisco (http://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf)*

such as Facebook and twitter are used to disseminate information and interact with citizens. Usage of cyberspace to deliver e-government services improves the relationship between the Government and society, allowing an open and transparent platform for political participation and expression. Parliament has online initiatives such as "***Botswanaspeaks"***, through which the electorates can raise their issues via ICTs and have Members of Parliament attend to them. Citizens can now interact with their political leaders and provide input on issues of National interest without the need to wait for ***"Kgotla***" meetings.

2.4 Risks and Threats

While ICTs have improved the lives of ordinary Batswana, there are risks and threats in the cyberspace that can potentially harm citizens. Because of its global connectedness, Internet has a wide range of risks and threats that go beyond Botswana's borders. The types of threats and risks range from relatively low level ones such as fake news to high level risks such as financial crimes and even interference of the country's ICT systems. There is, therefore, need for Batswana to be more vigilant and well informed on how they can protect their data in the cyberspace.

ICT enabled Critical National Infrastructure (CNI) such as electricity, water, transportation, telecommunications, commerce and health are susceptible to various cyber risks and threats since they rely on the Information and Communication Technologies (ICTs) to deliver their services. Cyber-attacks on CNI could have negative consequences for national security, the economy or the well-being of citizens of the country. This Strategy contains a series of measures and procedures to strengthen and have a coordinated approach to protect the Critical National Infrastructure against the risks and threats of the cyberspace.

Cybercrimes are not only from within the country, they are cross border. They may come from non-state actors (such as hacktivists who may not agree in principle with a position Botswana has taken or terrorists wreaking havoc on states that hold opposing views), state actors (countries with competing interest to those of Botswana or in conflict with Botswana) and organised crime. There is a broad spectrum of new challenging risks and threats in the cyberspace, which includes: cyber bullying, revenge porn, child pornography, identity fraud, or misuse of the Internet for extremism. Some cybercrimes are increasingly becoming common; these include distribution of sexual materials, child pornography, identity theft, recruitment into the use and distribution of illicit substances especially among minors, human. Multi-stakeholder cooperation between the governmental and relevant non-governmental bodies at national, regional and International level is essential in order to combat cyber threats as a whole and this Strategy advocates for that.

3.0 STRATEGIC FOUNDATIONS

3.1 Vision & Mission Statement

MISSION STATEMENT

Exist to protect information infrastructure, provide information security assurance, build capacity and capabilities to prevent and respond to cyber threats in order to enhance the socio-economic development of Botswana

3.2 Core Values

The core values represent the attitudes, behaviours and characters required to create an enabling and conducive environment for the successful realisation of the National Cyber Security Strategy objectives:

- **Accountability -** All organisations/institutions responsible for various strategic actions will make decisions in a responsible manner and utilise the resources efficiently and effectively**.**

- **Integrity** – The integrity of the infrastructure will be assured and data transmitted over the networks will not be altered or deleted without authority.

- **Confidentiality** – Privacy and fundamental rights of individuals will be preserved when implementing the various Cyber Security strategic initiatives and adherence to internationally acceptable governance principles will be maintained.

- **Collaboration -** Collaboration and cooperation will be established with all relevant multi-stakeholders including nationally and internationally institutions to share information and experiences in addressing Cyber Security challenges.

3.3 Strategic Objectives

Strategic Objectivel 1

To make Botswana more secure and resilient to Cyber attacks

Strategic Objective 2

To build Cyber Security capacity and capability in Botswana

Strategic Objective 3

To raise and promote Cyber Security awareness among the general public

Strategic Objective 4

To foster Cyber Security research and development

Strategic Objective 5

To enhance collaboration and cooperation on Cyber Security issues at national, regional and International level

Strategic Objective 6

To harness or leverage Botswana's Cyberspace for socio-economic development

3.4 Strategic Objectives and Initiatives

Strategic objectives and initiatives have been summarised in tabular form as shown below:

Strategic Objective: To achieve a secure and resilient Cyberspace			
Strategic Initiative	**Key Milestones**	**Expected Outcome**	**Responsibility**
1.1 Develop and review appropriate policies and legislation that promotes a secure cyberspace	1.1.1 Enact legislative, policy and regulatory framework for establishing National CIRT, National Cyber Security Operation Centre, Digital Forensic Labs and Research Centres.	Availability of appropriate legislation, policies and framework for relevant institutions	MTC, MDJS & AG
	1.1.2 Review and alignment of Cybercrime and Computer Related Crime Act.	Reviewed and aligned harmonised Cybercrime and Computer Related Crime Act	MDJS
	1.1.3 Review Cybersecurity related legislation to ensure protection of individual privacy and fundamental rights	Appropriate legislations that offer online protection	MITI, MTC, MDJS & AG
	1.1.4 Enact the Data Freedom of Information Laws	Enactment of Data Protection Freedom of Information Legislation	MNIG, MOPAGPA, AG
1.2 Establish a Botswana Computer Incidence Response Team (BWCIRT)	*1.2.1* Establish the National CIRT by acquiring the necessary technologies and resources. *1.2.2* Develop a framework which Defines the roles, responsibilities, powers, functions and resources for the operation of CIRT	Established and operational National CIRT Immediate Interim CIRT should be established as soon as possible	MTC, MDJS BOCRA
1.3 **Protect Critical**	*1*.3.1 Identify all Critical National Information	List of organisations/institutions	MTC, MDJS

National Information Infrastructure (CNII)	Infrastructure	which operate and manage CNII Register of CNII	
	1.3.2 Carry out a Cyber Security Audit on the management, operation and infrastructure to ensure CNII security and resilience	Generate Cyber Security Audit report	MTC, MDJS
	1.3.3 Assess and mitigate Cyber Security risks and threats on CNII and develop minimum security standards	Risk Assessment report and minimum security standards.	MTC, MDJS
1.4 Develop National Cyber Contingency Plans	1.4.1 Perform Cyber Security risk assessment and management	Cyber Security Risk assessment report	MTC, MDJS
	1.4.2 Develop Standard Operating Procedures (SOPs)	National Cyber Security Contingency plans of relevant CNIs Compiled Standard Operating Procedures	MTC, MDJS
	1.4.3 Develop coordination and response framework	National Coordination Framework developed	MTC, MDJS
1.5 Develop capability to host national Cyber Security drills/exercise	1.5.1. Identify processes, infrastructure and systems to be tested.	Identified systems, processes and infrastructure	MTC, MDJS
	1.5.2 Establish a cyber exercise planning team	Cyber exercise planning team formed	MTC, MDJS
	1.5.3 Conduct regular Cyber Security exercises / drills	Regular Cybersecurity exercises/drills	MTC, MDJS
1.6 Establish a Cyber Security Operation Centre	1.6.1 Establish baseline security requirements	Minimum security requirements	MDJS
	1.6.2 Establish incident reporting mechanism	Established and operational	MDJS

	for the Cyber Security Operation Centre	Cyber Security Operation Centre	
	1.6.3 Establish national and international cooperation		MDJS
1.7 Continuously monitor, analyse and manage the cyber threats and risks in Botswana	1.7.1 Continuously develop and improve national capacities and capabilities for forensic analysis	Improved forensic analysis capabilities.	MTC, MDJS
	1.7.2 Undertake regular testing to detect errors and vulnerabilities in CII	Security Audits and tests conducted to detect errors and vulnerabilities	MTC, MDJS
	1.7.3 Enhance and leverage national capability to undertake Cyber Security tests	Security Audits and Cyber Security testing Training programme	MTC, MDJS
	1.7.4 Develop and enhance capability and capacity to actively monitor cyber threats	Enhanced cyber threats monitoring capability	MTC and MDJS

Strategic Objective 2 :	**To enhance Cyber Security capacity and capability**		
Strategic Initiatives	**Key Milestones**	**Expected Outcome**	**Responsibility**
2.1 Building Cyber Security Capacity	2.1.1. Develop an operational cyber security capacity building framework.	Capacity building framework	MTC, MELSD, MoTE, Academia
	2.1.2 Establish Certification and accreditation for Cyber security experts	Internationally recognised Certification and Accreditation programme	MTC, MELSD, MoTE, Academia
	2.1.3 Promote and encourage the relationship between the academia and the industry on	Matched graduate skills with industry expectations	MTC, MELSD, MoTE, Academia

	cyber security.		
2.2 Continuously enhance the resilience, integrity and trustworthiness of all networks	2.2.1 Continuously develop the capacity of CIRT to reflect the ever changing technical and knowledge requirements resulting from the ever evolving cyberspace and ICTs	Cyber security capacity building plans for various levels CIRT (reviewed bi-annually)	MTC, MDJS
	2.2.2 Develop and recommend Cybersecurity frameworks, standards, procedures for institutions that own or manage NCI and the IIS to help manage Cyber security risks	CII Incident Reporting Procedures And Minimum security standards and procedures	MTC, MDJS
	2.2.3 Create/ continuously update Cybersecurity incidents register, assess incidents, and suggest measures to resolve issues and mitigate threats and risks	Real time Cyber security incident registers and measures to mitigate threats, risks and resolve incidents	MTC, MDJS
	2.2.4 Specify minimum log/ register requirements necessary for dependable Cybersecurity incident analysis	Dependable Cybersecurity incident analysis and findings log/register	MTC, MDJS
	2.2.5 Develop and recommend Cybersecurity frameworks, standards, procedures for non-CNII organisations to help manage Cybersecurity risks.	Minimum security standards and procedures	MTC, MDJS, MITI
2.3 Provide training that enhance capacities in cybercrime investigation and prosecution	2.3.1 Continuously develop the capacity of National Digital Forensics Lab (NDFL)	Fully operational digital forensic lab	MTC, MDJS
	2.3.2 Improve the capacities to investigate and prosecute cyber crime	Enhanced capabilities in digital investigation and prosecution	MDJS
	2.3.3 Develop courses and training programme on cybercrime for the justice system, law enforcement and personnel from other related agencies.	Effective Training programme on cybercrime investigation and prosecution	MDJS

	2.3.4 Promote continuous education of the justice system, law enforcement and personnel from other related agencies in the field of cyber crime	Continuous training programme for justice system and law enforcement staff	MDJS
	2.3.5 Develop digital forensics and evidence handling procedure and guidelines for the law enforcement agencies and personnel from other related agencies involved in the investigation and prosecution of cyber crime	Effective digital forensics evidence handling	MDJS

Strategic Objective 3 :	**To Promote Cyber Security Awareness**		
Strategic Initiatives	**Key Milestone**	**Expected Outcome**	**Responsibility**
3.1 Establish National, regional and international cooperation & collaboration on Cybersecurity awareness	3.1.1 Collaborate with relevant awareness & outreach entities	Effective exchange and use of information with collaborated institution	MTC, MoTE, MoBE, MELSD, MDJS, BWCIRT, Academia
	3.1.2 Establish a National body for cooperation & collaboration	Established cooperation & Collaboration Agreements with identified bodies	MTC, MoTE, MELSD, , MDJS, BWCIRT, Academia
3.2 Disseminate, collaborate and share information with all stakeholders	3.2.1 Develop & implement a communication plan	Effective awareness and education programmes Effective Communication Plan	MTC, MoTE, MELSD, MDJS, BWCIRT, Academia
3.3 Protect Children & other vulnerable groups against cyber threats & risks	3.3.1 Create an outreach programme for specific target groups	Effective information sharing mechanism	MTC, MoBE, MoTE, MDJS, BWCIRT, Academia
	3.3.2 Develop children Cyber Security	Availability of Children online	MTC, MoTE,

	protection guidelines	protection guidelines and adherence thereof.	MDJS, BWCIRT, Academia
3.4 Develop education and awareness to foster a culture of safe practices by users in relation to cyberspace	3.4.1 Develop ethical conduct guidelines on Cyber Security and promote its adoption	Availability of ethical conduct guidelines.	MDJS
	3.4.2 Integrate Cybersecurity education into training & learning institutions curriculum	Availability of Curriculum which includes Cybersecurity	MoBE, MELSD,, MoTE
	3.4.3 Implement a National Cybersecurity Outreach for all other groups	Implementation of National Cybersecurity Outreach Programme	MTC, MDJS, BWCIRT
	3.4.4 Develop and implement an awareness raising strategy to raise awareness among the general public	Developed (Effective) Cybersecurity awareness strategy	MTC, MDJS, BWCIRT
	3.4.5 Promote a culture for the adoption of Cybersecurity awareness	Informed society on cyber Security	MTC, MDJS, BWCIRT

Strategic Objective 4 : To Foster Cyber Security Research and Development			
Strategic Initiatives	**Key Milestone**	**Expected Outcome**	**Responsibility**
4.1 Develop a national Cyber Security research,	4.1.1.Establish a Cybersecurity research institution	Operational Cybersecurity research institution	MTC, MoTE, MELSD, MDJS, BWCIRT,

development, and innovation agenda			Academia
	4.1.2.Undertake periodic Cybersecurity research to inform awareness & education programmes	Well researched Cybersecurity research education material	MTC, MoTE, MELSD, , MDJS, BWCIRT, Academia
	4.1.3.Examine options to better inform and educate the community on a broad range of cyber risks and threats	Adoption of awareness/outreach research projects	MTC, BWCIRT
	4.1.4.Assess, evaluate and monitoring community awareness on cyber threats & risks	Cybersecurity Awareness Assessment Report	MTC, ,BWCIRT
4.2 Establish a Cybersecurity centre of excellence	4.2.1 Establish a framework for excellence in Cybersecurity	Cybersecurity excellence Framework	MTC, MoTE, MELSD, MDJS, BWCIRT, Academia
	4.2.2 Facilitate formation of Research focussed Groups that address Cybersecurity threats and risks	Research Focussed Groups	MTC, MoTE, MDJS, BWCIRT, Academia
	4.2.3.Enhance Cybersecurity expertise through research and innovation	Enhanced Cybersecurity expertise	MTC, MoTE, MDJS, BWCIRT, Academia
	4.2.4 Promote collaboration between research institutions, industry, BWCIRT and government and provide necessary incentives.	Informed society on Cybersecurity	MTC, MDJS, MoTE, MoBE, BWCIRT, Academia, MELSD, Business Botswana,

Strategic Objective 5 : To enhance stakeholder collaboration and cooperation on Cyber Security issues at national, regional and International levels			
Strategic Initiatives	**Key Milestone**	**Expected Outcome**	**Responsibility**
5.1 Enhance information	5.1.1 Establish an Information sharing	Effective exchange of	MTC, MDJS,

sharing and cooperation	Framework that fosters both public and private collaboration	information with collaborated institution	BWCIRT, Academia
	5.1.2. Identify and review existing collaborations with countries/organisations on cybersecurity.	Established cooperation & Collaboration Agreements with identified bodies	MTC , MDJS, BWCIRT, Academia
	5.1.3. Enter into bilateral/multilateral treaties, agreements and conventions on cybercrime and cyber security.	Effective Bilateral and multilateral agreements	MTC , MDJS, BWCIRT
5.2 Promote national, regional & international collaboration and information sharing on Cybersecurity	5.2.1 Participate in national, regional & international discussions and share information at the same fora on Cybersecurity activities	Knowledge and information sharing	MTC, MDJS, BWCIRT, Academia

Strategic Objective 6 : To harness or leverage Cyberspace for socio-economic development			
Strategic Initiatives	**Key Milestone**	**Expected Outcome**	**Responsibility**
6.1 Raise Cybersecurity awareness among decision makers, policy makers and political leaders.	6.1.1. Include Cybersecurity issues in the High-Level Consultative Forums (fora).	Well informed leadership on Cybersecurity issues	MTC, MOPAGPA, & MDJS, Business Botswana
	6.1.2. Host a high-level annual Cybersecurity summit where Government and Business leaders discuss Cybersecurity issues and trends and drive this Strategy's implementation.	High-level Cybersecurity summit	MTC, MOPAGPA, & MDJS, Business Botswana
	6.1.3. Advocate for an open, free, secure and safe use of the cyberspace.	Effective and responsible use of the cyberspace	MTC, MOPAGPA, & MDJS
	6.1.4 Enhance dissemination of public services in a safe and secure cyberspace environment	Availability of secure e-services	
6.2 Enhance public private partnership to promote security and resilience in cyberspace infrastructure, networks, products and services	6.2.1 Facilitate the adoption and use of secure e-commerce transactions and platforms	Availability of cyber secure e-commerce platforms	MTC, MITI, Business Botswana
	6.2.2 Assist and promote the development of local Cybersecurity products and services.	Effective information sharing mechanism Availability of cyber secure local products and services.	MTC, MITI, MDJS,
	6.2.3. Promote the use of secure electronic signature to secure electronic transaction.	Availability of public key infrastructure (PKI) Increased use of secure electronic signature in electronic transactions.	MTC, MITI , BOCRA

	6.2.4 Promote investment on Cybersecurity innovations and support commercialisation of research products and services.	Well defined programmes for support investment on R & D products and services	MTC, MITI, MDJS,
	6.2.5 Develop policies and practice that will ensure Cybersecurity consideration are built into public and private partnership such as procurement	Secure e-procurement strategy that promote public private partnership	MITI, PPDAB, Business Botswana

4.0 IMPLEMENTATION

4.1 Critical Success Factors

The successful implementation of this strategy will broadly depend or be influenced by the following considerations:-

- **High-level ownership** - It is essential that this strategy is endorsed by and driven from the highest body in Botswana and that it receives the full executive support in order to be successfully implemented. The National Executive should identify national business priorities and provide monetary and human resources needed to implement the strategy. In addition, the importance of this strategy needs to be understood across all sectors.

- **Cybersecurity Risk Assessment** - The incorporation of risk management as a delivery area within the executive management (both public and private enterprises) provides a strong foundation for Cybersecurity implementation—covering the areas of people, process and technology. The security of digital infrastructure and information must be understood as vital and incorporated within all organisational functionality beyond technical solutions.

- **Resource Prioritisation** - Identification and prioritization of key resources aimed at improving the country's security, resilience, operational capacities to effectively manage and respond to cyber incidents as well as protect against ever persistent threats is crucial. Embedded within this area is the need to continuously improve operational capabilities to keep abreast with the level of sophistication of cybercrime as well as advanced persistent threats.

- **Human Capital** - Efficient implementation of Cybersecurity requires highly qualified and skilled human resource across all sectors. The ability of institutions in both Public and Private sector to attain and retain skilled human resource is therefore important for maintaining and ensuring a strong protection approach against cyber threats especially with operators of Critical National Infrastructure (CNI).

- **Multi-stakeholder Approach** - Managing compliance of all key stakeholders and actors within both the public and private sector provides assurance on improving the nation's Cybersecurity maturity. This requires deliberate effort and initiative from each stakeholder to meet their obligations. A proper coordination of efforts is required with a view to conducting cyber drills among sectors and to ensure that national response and sector response are coordinated. Information sharing is also

key. The ability to build trust and relationships with key stakeholders (industry, international Cybersecurity organizations and sovereign states) is important due to the fact that cyber threats span various jurisdictions.

- **International Cooperation** - The nature of cyber space is borderless and complex; this implies that managing risk is a shared responsibility beyond Government alone. Various key players besides GoB including NCII operators, businesses, private sector, academia, civil society and citizenry should share this responsibility based on harmonious collaboration. International collaboration is therefore key in ensuring presence of capacity and mechanisms to handle cyber threats from a foreign adversary as well as provide assistance to international allies when required.

4.2 Governance Framework

There shall be a governance structure, which will oversee the implementation of the National Cyber Security Strategy. It is recommended that a multi-stakeholder National Cybersecurity Advisory Council (NCAC) , comprising representatives from the private sector and relevant Government institutions and agencies, should be established. The Advisory Council will oversee the operations of Botswana Computer Incidence Response Team (BWCIRT) and overall implementation of the National Cybersecurity Strategy. The BWCIRT will act as the Secretariat of the National Cybersecurity Advisory Council.

In addition it is also recommended that a specialised function, separate from mainstream BWCIRT duties, of a Cybersecurity Operation Centre (COC) be established in order to ensure that the country is well prepared for all Cyber threats. The COC should deal with the threats and attacks of the highest level. These should be those attacks, the objective of which threatens the security, sovereignty and economy of the republic of Botswana. Such threats could be either state sponsored (such as espionage, cyber conflict) or non-state actor activities such as terrorism. Because of the nature of its assignment, COC should be established and managed by the National Security agencies.

The strategy also recommends the establishment of Digital Forensic Laboratory (DFL) to assist with processing and analysis of the electronic evidence. It is recommended that Botswana Police Service is mandated to take the lead in establishment of the DFL.

Various sectorial CIRTs may also be established in order to assist the various sectors in responding to the Cyber Security challenges. The coordination and sharing of information of the sectorial CIRTs will be done through the BWCIRT.

The diagram below summarises the proposed governance structure for the implementation of the National Cybersecurity Strategy:

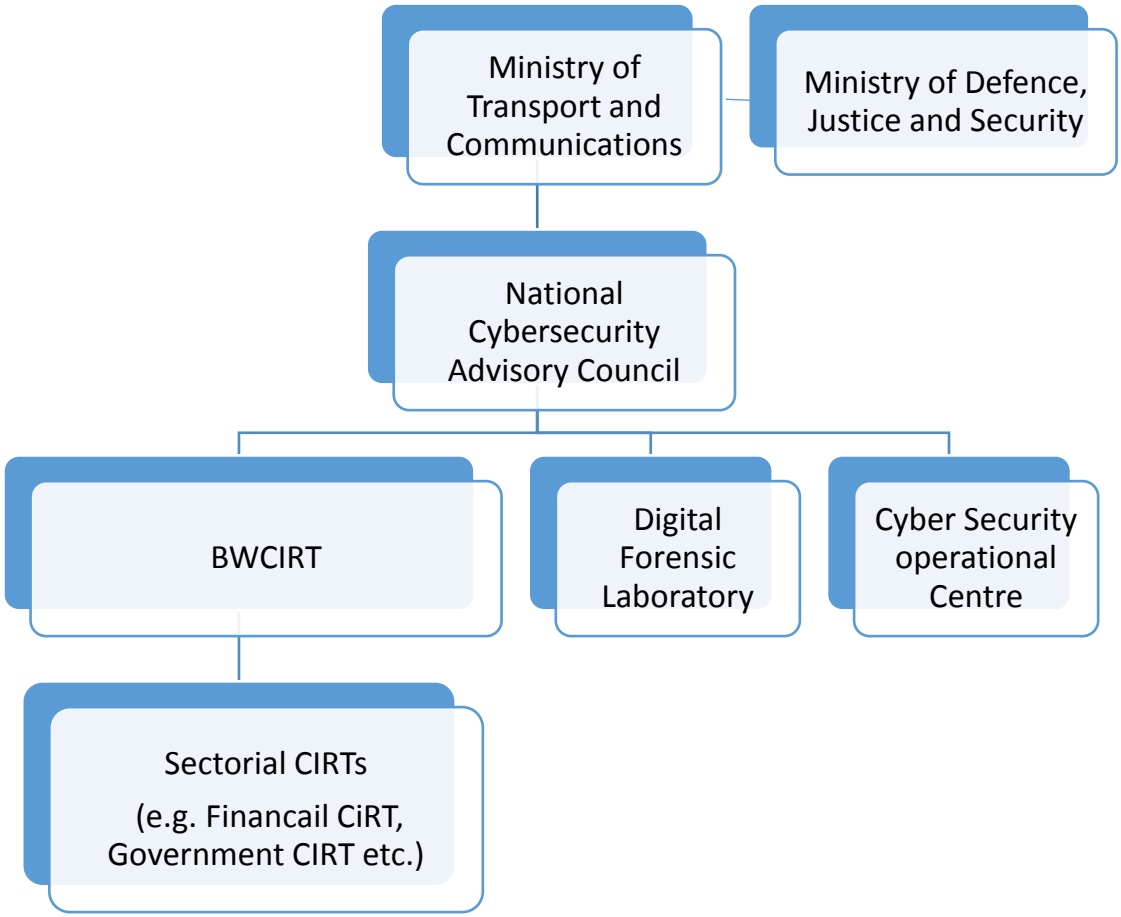

Figure 1 : NCS Governance Structure

4.3 Roles and Responsibilities

The role of Government in Cybersecurity is extensive;this is to be expected given the vital role of ICTs in the nation, the wide range of threats and vulnerabilities and the cross-sector nature of Cybersecurity. The Government will assume a variety of roles including national level policy-making and citizen level capacity-building. However, it should be noted that cybersecurity is everyone's responsibility. Various stakeholders, particularly private and independent sectors, play a leading and key role in ensuring security in the cyberspace.

4.3.1 Ministry of Transport and Communications

The Ministry of Transport and Communications (MTC) is responsible for developing relevant policies and strategies, and supports the development of relevant laws

governing the ICT sector in Botswana. It also coordinates their implementation through National, regional and global collaborative efforts that harness local resources, talent and innovation. Equally, MTC is responsible for the general oversight of the ICT sector including cybersecurity. This role was further pronounced through a recent Presidential directive, giving MTC the mandate for the overall coordination and oversight of ICT, through its ICT roadmap. This was a direct result of consultation and participation of the different Ministries, which supported this clarification of roles for the ICT sector.

4.3.2 Ministry of Defence Justice and Security

The Ministry of Defence Justice and Security (MDJS) is responsible for ensuring the safety and security of the country, both in the physical space and in the cyberspace. The Ministry and its various agencies continually assess the cyberspace landscape to identify threats and risks to Botswana's National Security and work together with Law Enforcement Agencies (LEAs) and other security services to combat cyber terrorism and maintain law and order during nationwide cyber-attacks or emergencies. The Ministry is responsible for overseeing the justice system and law enforcement of Cybersecurity related laws, and would play a key role in the fight against cybercrime, especially investigation detection, and prosecution. In addition the judiciary also has to be kept abreast about the latest challenges and development on Cybersecurity for appropriate justice to be dispatched. Criminal laws, procedures and policies needs to be constantly updated to address Cybersecurity incidents and respond to cybercrime.

4.3.3 National Cybersecurity Advisory Council

The coordination and implementation of Botswana's National Cybersecurity Strategy (NCS) would be led by the proposed National Cybersecurity Advisory Council (NCAC) in collaboration with the relevant Ministries, Agencies or Departments. The central coordination is cognisant of public private partnerships towards ensuring a robust national Cybersecurity approach. NCAC will provide strategic leadership for the BWCIRT. The key stakeholders that will be represented in the National Cybersecurity Advisory Council are:

a) Ministry of Transport and Communications
b) Ministry of Justice Defence and Security
c) Law Enforcement Agencies
d) BOCRA
e) Non-banking financial institutions
f) Banking institutions
g) Public Telecommunications Operators
h) Internet Service Providers
i) National Critical Infrastructure Providers
j) Academia
k) Consumers

l) ICT Industry

4.3.4 National Computer Incident Response Team (BWCIRT)

The role of the proposed National CIRT is to act as the trusted point of contact as well as provide central operational coordination for incident response at National level. This entails ensuring partnership with international CIRTs to ensure presence of mechanisms for cross-border incident handling as well as coordinating all sector specific country response teams. Taking into consideration that Cybersecurity issues are increasing and that it may take a long time for the realisation of some of the strategic actions and approval of the strategy, it is recommended that as a matter of urgency the country starts with the National CIRT so that it can assist in monitoring the cyber threats and consumer awareness**.**

The main responsibilities of the National CIRT cover amongst others the following areas:

i) Providing incident response support to all relevant stakeholders via established, trusted, authorised and centrally coordinated initiatives at the national level;
ii) Dissemination of critical information such as early warnings and alert notifications, security advisory, and upholding security best practices;
iii) Acting as a single point of contact for cyber incident reporting and coordination;
iv) Detecting and identifying anomalous activity;
v) Analysing cyber threats and disseminating cyber threat warning information;
vi) Analysing and synthesizing incident and vulnerability information disseminated by others such as vendors to provide an assessment for interested stakeholders;
vii) Establishing trusted communications mechanisms and facilitating communications among stakeholders to share information and address cyber security issues;
viii) Developing mitigation and response strategies and coordinating incident response;
ix) Sharing data and information about the incident and corresponding responses;
x) Coordinating international cooperation on cyber incidents; and Building capacity in all the above areas using advanced technology and techniques, establishing methods, and researching threat analyses and mitigations.

4.3.5 Law Enforcement Agencies

Law Enforcement Agencies (LEA) and Security Forces play a key role in investigating cybercrimes and enforcing Cybersecurity related laws. They also play a vital role in ensuring collaboration with a wide range of partners to combat cybercrimes with international dimensions and/ or span multiple jurisdictions. Further, these agencies play a vital role in keeping law and order during nation-wide cyber-attacks and

emergencies. The law enforcement agencies will establish collaboration with international institutions such as Interpol and the Virtual Global Taskforce (VGT) on child abuse material to address Cybersecurity.

4.3.6 Regulatory Authorities (BOCRA, NBIFIRA, Bank of Botswana etc.)

The regulators are mainly responsible for the consumer protection, therefore it will play an important in the implementation of the national Cybersecurity strategy. For example BOCRA provides regulatory oversight over the communications sector as aligned to the MTC policy direction. Further, BOCRA, in collaboration with MTC, ensures compliance within the communications sector; that operators adhere to national Cybersecurity laws, policies and standards

4.3.7 National Critical Information Infrastructure Owners

NCII owners are keys to Botswana's efforts to maintain Cybersecurity as they continually assess and address threats and vulnerabilities as well as ensure various mitigation measures are well implemented. They also ensure compliance with relevant National Cybersecurity laws, policies, standards, procedures, frameworks, etc.

The following sectors are identified as national critical infrastructure sectors with regard to the cybersecurity: ***finance, communications, energy, water, emergency services, food, public safety, health, public services*** and ***e-government***

4.3.8 Consumers & General Public

Effective implementation of security at individual level involves some level of understanding with cyber security threats (e.g. viruses, spam, etc.) and the adoption of appropriate technical safeguards (e.g. updating anti-virus software, firewalls, etc.). The national cybersecurity strategy has to focus on the dissemination of appropriate basic cybersecurity awareness information to the general public. For example consumers have to be made aware that they cannot share information such as password, PIN, online with unknown persons and regularly they have to change their passwords and update the anti-virus.

4.3.9 Service Providers

The regulator (BOCRA) has to ensure that service providers implement appropriate technical measures, procedures and standards to enhance the information security through their networks. A cybersecurity technical measures framework needs to be developed and implemented that would incorporate technical (e.g., standards, software), procedural (e.g., guidelines, standards, or mandatory regulations) and

personnel (e.g., best practices) safeguards. For example measures may include promoting government and private sector to adopt international standards related to cyber security (e.g., ISO 27001 on Information Security Management System).

4.3.10 Academia

Academic institutions will play an important role in the implementation of the national cybersecurity strategy. Academic institutions educate the technical, management and information assurance experts required to execute cyber security strategies. In addition, research and development (R&D) activities, need to be carried out on cybersecurity and the protection of information infrastructures. Through partnerships with the private sector and governments the Academia can assist in the development of cybersecurity related technologies, techniques, standards and processes that further the national cybersecurity agenda. The Academia institutions may also have cybersecurity forensics laboratories which may assist on the investigation and enforcement of cybersecurity legislations

4.3.11 Civil Society

Civil society will play an important role in ensuring that there is a right balance in terms of protection civil liberties, privacy and human rights etc. as we implement the national cyber security strategy. The civil society needs to form part of the stakeholders in order to provide confidence and integrity that the national cybersecurity strategy implementation does not tramp on civil liberties. For example monitoring cyberspace has to be done in a manner which does not invade personal privacy. Internationally a number of civil society not-for profit organisations have also been established around the issue of cybersecurity and cybercrime for example those dealing with child online protection (COP). Therefore it is very important that collaboration is established with international civic society to assist also on the consumer education.

4.3.12 Private Sector (Industry)

Businesses are expected to implement an adequate level of cyber security safeguards into their business operation and practices. Such safeguards typically involve the installation of technical solutions and the adoption of best practice secure business processes. For example, the financial and banking sector, with its dependency on international clearing and central banking, and its links to international financial market systems, cyber security concerns should be accorded high priority.

On a collective level, the private sector has an important role to play in its own right and in cooperation with government in developing cyber security business norms, standards and codes of conduct, as well as in identifying and encouraging the adoption of good practices. By taking part in relevant forums or standards-development

organizations, industry plays a critical role in agreeing on technical standards to protect security.

Equipment suppliers within the cyber security defence industry provide technical solutions towards protection of digital infrastructure and information. The specific role for vendors is to cooperate with the Botswana's National CIRT (BWCIRT) in providing vulnerability information These would help support incident response and ensure compliance with the minimum cybersecurity standards for vendors' products and services..

4.4 Funding Resources

Funding and adequate resourcing will be fundamental to the implementation of this strategy. Given that cybersecurity is a key to the realisation of Botswana's goals and vision, the government and the private sector should ensure that National Cybersecurity Strategy and implementation programmes are adequately funded and resourced. Funding of International cooperation partners should also be sourced to assist with the implementation of the strategy recommendation. Establishment budget estimate at a high-level is summarised in the table below:

Table 1 : NCS Establishment Budget

Budgetary Activities	**Estimated Amount**
Establishment of CIRT	
Phase 1: Basic CIRT services	P5 Million
Phase 2: Enhanced CIRT services	P3 Million
Phase 3: Advanced CIRT Services	P 2 Million
Sub-total for BWCIRT	**P 10 Million**
Establishment of cybersecurity operation centre	P15 Million
Capacity building programmes	P 15 Million
Consume awareness programs	P 5 Million
Digital forensic laboratory	P 16 Million
Cybersecurity Research programme	P 4.5 Million
TOTAL	**P65.5 Million**

4.5 Monitoring and Evaluation

Until National Cybersecurity Advisory Council (NCAC) is established MTC and BOCRA could collaborate and employ the approaches mentioned below to develop and provide a comprehensive Monitoring and Evaluation (M&E) framework. Once the NCC is established, NCC in coordination with MTC will provide operational monitoring and evaluation for the implementation of this strategy.

A comprehensive Monitoring and Evaluation (M&E) framework shall be developed to determine the long-term impact and outcome of the strategy across all sectors based on periodic reviews (which would include a midterm review at the 3 year milestone and a long term review at the 5 year milestone). The M&E framework shall consider the following areas:

- Alignment to Government of Botswana performance assessment approach;
- Use of an external evaluator to undertake the long-term impact assessment (at 5 years); and
- Assessment of the progress towards attainment of level 5 of the Cybersecurity Capability Maturity Model.

The key elements of the M&E approaches are:

- Setting performance targets for various ministerial or governmental departments, groups or individuals responsible for specific aspects or actions of the strategy;
- Establishing performance plans which establish a common understanding of what is to be achieved, how it is to be achieved and managing resources to guarantee success in implementation;
- Monitoring and reporting performance;
- Evaluating departments, groups or individual performance against established performance targets.

GLOSSARY

Critical Information Infrastructure refers to the digital infrastructure whose disruption or damage negatively affects the well-functioning of the economy.

Cyber attack is an attempt by hackers or malicious actors to damage or disrupt the normal functioning of a computer network/ system/ application.

Cyber crime refers to crime that involves use of a computer and/or network. It could either be in an instance where a computer is used in the commission of crime or where the computer is the target of the crime.

Cyber terrorism refers to the politically or socially motivated use of ICT to cause harm or fear within a society.

Cyber Security culture is a term that broadly refers to the alignment of cyber security with the organization's goals to create a holistic environment of trust and achievement of consistent results. It involves the continuous assessment of risk to create a resilient ICT environment.

Cyber Security is a term that describes the protection of ICT systems from damage, theft or disruption of the processes they run. It encompasses the combination of people, process and technology.

Cyber Security maturity is a description of how an organisation quality-assures its cyber security implementation and management and measures how practices are approached as well as sustained to create value.

Digital Infrastructure refers to interconnected computers, systems/applications and networks to support information sharing, processing and storage.

e-Commerce refers to the business that are done electronically, including the sharing of standardised unstructured or structured business information by any electronic means.9

e-Government broadly refers to the use of ICT to improve service delivery as well as improve productivity within Government.

e-Health refers to health services and information delivered or enhanced through the Internet and related technologies.

Netiquette refers to the rules of etiquette that apply when communicating over the Internet or social networks or devices. It is a social code of network communication.

Public Key Infrastructure is a term used to describe the laws, policies, procedures, standards, and software that regulate and control secure operations of information based on public and private keys.