National Cybersecurity Policy and Strategy
2020

TABLE OF CONTENTS

FOREWORD BY THE MINISTER

Protecting Papua New Guinea's national security and promoting the prosperity of the PNG Citizen are among my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors. Cyberspace is an integral component of all facets of our new digital economy, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and hackers have increased the frequency and sophistication of their malicious cyber activities. We must make sure to secure and preserve cyberspace for future generations.

Information and communication technology (***ICT***) is an integral part of public administration, global trade and social interaction in today's world. Major economic partners such as APEC are focusing on e-Trade and e-Commerce, as governments across the region set their agenda on implementing e-Government. The 2018 APEC theme which centred around "Harnessing Inclusive Opportunities, Embracing the Digital Future", is at the forefront of the Government's vision for socio-economic development in the country.

Papua New Guinea's success depends on its ability to harness these technological advances to drive economic growth and raise productivity and living standards for all Papua New Guineans. A key focus of the government's digital transformation efforts of government is ensuring PNG keeps pace with community needs and expectations

The digital economy is fundamentally changing how Papua New Guineans live, work and interact with Government. The PNG public expects government services to be simple, easy and fast to use. To meet these expectations we must be innovative, practical and user-centred in our work. Cyber-related risks are evolving rapidly as PNG becomes increasingly reliant on ICT, as such, it is of paramount importance that PNG's technical and intelligence capabilities must also be developed to international standards and in accordance with international best practice to protect PNG's critical infrastructure systems and essential services. If these cease to function or our compromised, our Government, economy and society can be adversely affected.

The National Cyber Policy demonstrates the GoPNG's commitment to strengthening the Government of PNG's cybersecurity capabilities and securing PNG from cyber threats. It is a call to action for all PNG Citizens, our universities and all educational institutions, all branches of Government, the private sector, civil society, and the Technical Communities to take the necessary steps to enhance our national cyber-security.

To support the Government's drive towards digital economy, current government policy encourages competition through the use and development of ICT. As a result, ICT activities in the country have increased significantly and have impacted immensely on society. However, the use of ICT poses risks to the security of electronic systems and infrastructure. These risks are appropriately addressed through the enhancement of Cybersecurity.

Cybersecurity is a fundamental and integral component of ICT development. Cyber-related risks are evolving rapidly and as our country becomes increasingly reliant on ICT, it is of paramount importance that our technical and intelligence capabilities in Cybersecurity must also be developed to international standards and in accordance with international best practice in order to provide adequate protection for our critical infrastructure systems. When our critical infrastructure systems or essential services do not function properly, our Government, economy and society can be adversely affected.

Recent technological progress has for instance, enhanced the level of convenience with which we conduct our business and carry out daily tasks that previously required cumbersome physical

attendances and manual processes. The internet of things (***IoT***) has simplified such processes as computers have now replaced most of these functions. We are now able to purchase electricity on mobile platforms, airplane tickets online and perform numerous tasks from the comfort of our homes.

To be prepared for the compounded risks associated with the increased dependence on the use of ICT, this National Policy Framework helps define how Cybersecurity-related activities should be organized and how roles and responsibilities should be shared among institutions. In particular, the Policy provides for the establishment of PNG's technical and intelligence capabilities and our collaboration with other governments and similar regional and international establishments, in our efforts to protect our critical infrastructure and systems.

Moreover, to manage cyber threats, appropriate laws and structures must be developed to address incident management. This Policy provides for relevant legislation, regulations and guidelines to be developed and the establishment of organisations to support Cybersecurity initiatives and enable the Government to assume the lead role in ensuring a safe and secure cyber environment.

The successful implementation of this Policy hinges on effective coordination amongst the implementing agencies and sufficient and sustainable resourcing through Government and industry commitment. The onus is on the lead implementing agencies to develop appropriate strategies and advise the Government from time to time to commit necessary resources.

The Policy will be reviewed from time to time to ensure its objectives continue to be relevant and commensurate with the fast advancing pace of technological development.

HON. TIMOTHY MASIU, MP
Minister for Communications and Information.

ABBREVIATIONS

APEC	Asia Pacific Economic Cooperation
APNIC	Asia Pacific Network Information Centre
ASMS	Automated Spectrum Management System
CBD	Central Business Districts
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIRT	Computer Incidents Response Team
COPWG	Child Online Protection Working Group
CSIRT	Computer Security Incidents Response Team
CSOC	Cybersecurity Operations Centre
DCI	Department of Communications and Information
DDOS	Distributed Denial of Service
DFA	Department of Foreign Affairs
DJAG	Department of Justice and Attorney General
GCA	Global Cybersecurity Agenda
ICT	Information and Communication Technology
IFMS	Integrated Financial Management System
IGIS	Integrated Government Information System
IoT	Internet of Things
ISO	International Standards Organisation
ITU	International Telecommunications Union
LNG	Liquefied Natural Gas
MDGs	Millennium Development Goals
NCPISC	National Cybersecurity Policy Implementation Steering Committee
NCSC	National Cybersecurity Centre
NCSAC	National Cybersecurity Strategic Advisory Committee
NICTA	National Information and Communications Technology Authority
NID	National Identification
NIO	National Intelligence Organisation
NISIT	National Institute of Standards and Industry Technology
NSAC	National Security Advisory Committee
NSA	National Security Agency
NSC	National Security Council
OCC	Office of Chief Censor
OSCA	Office of Security Coordination Authority
PNGCERT	Papua New Guinea Computer Emergency Response Team
PNGDF	Papua New Guinea Defence Force
PPP	Private Public Partnership
RPNGC	Royal Papua New Guinea Constabulary
SDGs	Sustainable Development Goals
UN	United Nations
UNGA	United Nations Global Agenda

1.0 BACKGROUND

Protecting Papua New Guinea's national security and promoting the prosperity of the PNG Citizen are among my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors. Cyberspace is an integral component of all facets of our new digital economy, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and hackers have increased the frequency and sophistication of their malicious cyber activities. We must make sure to secure and preserve cyberspace for future generations.

The digital economy is fundamentally changing how Papua New Guineans live, work and interact with Government. The PNG public expects government services to be simple, easy and fast to use. To meet these expectations we must be innovative, practical and user-centred in our work.

Papua New Guinea's success depends on its ability to harness these technological advances to drive economic growth and raise productivity and living standards for all Papua New Guineans. A key focus of the government's digital transformation efforts of government is ensuring PNG keeps pace with community needs and expectations

The ability for citizens, the government, and the private sector to connect to their counterparts in other countries through the Internet has been enhanced with the commissioning of the Coral Sea Cable between Australia and Papua New Guinea.

Domestic fibre network connectivity between provinces means that citizens and government and the private sector across provincial towns and cities have just as efficient broadband connectivity inter-province and with counterparts overseas.

But as the Internet becomes more accessible and affordable, issues pertaining to cyber safety, cyber security, and cybercrime have emerged and require immediate policy and operational intervention to ensure the safety of all citizens, their personal data and the data stored and collected by the Government.

Cyber-related risks are evolving rapidly as PNG becomes increasingly reliant on ICT, as such, it is of paramount importance that PNG's technical and intelligence capabilities be developed to align it with international standards/norms and in accordance with international best practices to protect PNG's critical infrastructure systems and essential services. If these cease to function or are compromised, our Government, economy and society can be adversely affected.

Information and communication technology (***ICT***) is an integral part of public administration, global trade and social interaction in today's world. Major economic partners such as APEC are focusing on e-Trade and e-Commerce, as governments across the region set their agenda on implementing e-Government. The 2018 APEC theme which centred around "Harnessing Inclusive Opportunities, Embracing the Digital Future", is at the forefront of the Government's vision for socio-economic development in the country.

New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the citizens of PNG people to thrive.

Protecting Papua New Guinea's national security and promoting the prosperity of the PNG Citizen are among my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors.

Cyberspace is an integral component of all facets of our new digital economy, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and hackers have increased the frequency and sophistication of their malicious cyber activities.

The global COVID-19 pandemic that hit every corner of the world forced all Papua New Guinea citizens and the Government to reimagine our society and reinvent the way we work and live. During the lockdown, people turned to Internet to get work done, for shopping, working and even learning; However, at the same time cybercriminals took advantage of the lack of cyber hygiene by many PNG citizens and began aggressively targeting people.

PNG Citizens were not alone in seeing this significant rise in cybercrime, it remains a world-wide phenomenon. Illegal and harmful content aimed at children multiplied as more people went online during lockdown. The COVID-19 crisis showed us how criminals actively take advantage of society at its most vulnerable, this opportunistic behaviour of criminals should not overshadow the overall threat landscape.

Criminals use innovative methods to increase the volume and sophistication of their attacks, and inexperienced cybercriminals can carry out phishing campaigns more easily through crime as-a-service. Criminals quickly exploited the pandemic to attack vulnerable people; phishing, online scams and the spread of fake news became an ideal strategy for cybercriminals seeking to sell items they claim will prevent or cure COVID-19.

Cyber-attacks have become more sophisticated, targeting specific organisations in the public and private sector through victim reconnaissance. COVID-19 pandemic has triggered a significant increase in cybercrime.

1.1 DEFINITIONS

Cybersecurity refers to the assortment of tools, policies, security concepts and safeguards, guidelines, risk management practices, activities, training, best practices, assurance and technologies that can be used to protect cyberspace, organisational and user's assets, including, interconnected electronic devices, personnel, infrastructure, applications, services, telecommunications systems, and the entire information transmitted and or stored in the cyber-environment.[1]

Cybersecurity is the practice of defending computers and servers, mobile devices, electronic systems, networks and data from malicious attacks. It is also known as information technology security or electronic information security.

Cyber-security is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. Cyber-security relies on cryptographic protocols used to encrypt emails, files and other critical data. This not only protects information that is transmitted but also guards against loss or theft. End user security software scans computers for pieces of malicious code, quarantines this code and then removes it from the machine.

Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet. These tactics are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites; malicious software that can infect and inherently damage systems; and identity theft by hackers who steal personal data such as bank

[1] *A Definition of Cybersecurity – ITU http://www.itu.int*

account information and credit card numbers. Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.

Cyber Safety is the safe and responsible use of information and communication technology. It is about practicing effective cyber hygiene and ensuring that all information is kept safe and secure.

Cyber safety is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums. Without proper knowledge or education their identity can be stolen or compromised. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen.

Typical lapses in cyber safety result in a number of possible scenarios, such as:

- Phishing: An Internet hacking activity used to steal secure user data, including username, password, bank account number, security PIN or credit card number.
- Pharming: An Internet hacking activity used to redirect a legitimate website visitor to a different IP address.
- Spyware: An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.
- Malware: An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

Cyber ediquette is about being responsible with that information, being respectful and civil of other people online privacy and their beliefs, and using good ‘netiquette’ (internet etiquette).

As information infrastructure and internet became more complex it has became critical to maintain systems and keep them secured and running all the time. In recent years, all systems were and continue to be exposed to external attacks introduced through the Internet.

The most difficult challenge today in cyber security is the ever-evolving nature of security risks themselves from ransomware, malware, identity theft, fraud, phising, pharming, spyware, the list continues

Cybercrime is any criminal activity that involves a computer, networked device or a network. Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may target private personal information, as well as corporate data for theft and resale.

The Council of Europe’s Convention on Cybercrime, also known as the Budapest Convention, defines cybercrime as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements.

Other forms of cybercrime include illegal gambling, the sale of illegal items, like weapons, drugs or counterfeit goods, as well as the solicitation, production, possession or distribution of child pornography.

Crimes typically cluster around the following categories:

- Crimes against the confidentiality, integrity and availability of computer data and systems;
- computer-related crimes;
- content-related crimes;

- crimes related to infringements of copyright and related rights.

Most cybercrimes are carried out with the expectation of financial gain by the attackers.

- Cyberextortion, is crime involving an attack or threat of attack coupled with a demand for money to stop the attack, for example--Ransomware
- Ransomwear--a form of cyberextortion in which the victim device is infected with malware that prevents the owner from using the device or the data stored on it. To regain access to the device or data, the victim has to pay the hacker a ransom.
- Cryptojacking, uses scripts to mine cryptocurrencies within browsers without the user's consent
- Identify theft, occurs when an attacker accesses a computer to glean a user's personal information that they can then use to steal that person's identity or access bank or other accounts.
- Credit card fraud, occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on darknet
- Cyberespionage--occurs when a cybercriminal hacks into systems or networks to gain access to confidential information held by a government or other organization

Cybercrime is any criminal action which can occur in the offline world but has been facilitated by ICT. This typically includes online frauds, online gambling, money laundering, and any sex crimes.

Cyber resilience refers to an entity's ability to continuously deliver the intended outcome, despite adverse cyber events. It is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Cyber resilience focuses on the preventative, detective, and reactive controls in an information technology environment to assess gaps and drive enhancements to the overall security posture of the entity.

Cyber resiliency concerns the assurances for a nation that its critical infrastructures will remain effective and operational for it to endure inevitable attacks.

Critical infrastructure top targets

- Public/government
- Telecommunications
- Health
- Academic
- Manufacturing
- Power/utility, and
- transportation
- General information warfare threats

While cyber security is foundational to protect assets from an attack happening in the first place. Cyber resiliency concerns the assurances for a nation that its critical infrastructures will remain effective and operational for it to endure inevitable attacks.

Attribution of responsible attackers is a capability enabled by threat intelligence analysis of multiple sources of information to learn tactics, techniques, and procedures used by attackers. This information enhances methods for security and resiliency.

Transparency of these capabilities, propensity for risk, and cultures are challenges to national cyber strategies being comparable to protect our tightly woven digital economies.

Cybersecurity procedures explain the rules for how employees, consultants, partners, board members, and other end-users access online applications and internet resources, send data over networks, and otherwise practice responsible security. Typically, the first part of a cybersecurity policy describes the general security expectations, roles, and responsibilities in the organization. Stakeholders include outside consultants, IT staff, financial staff, etc. This is the "roles and responsibilities" or "information responsibility and accountability" section of the policy.

The policy may then include sections for various areas of cybersecurity, such as requirements for antivirus software or the use of cloud applications.

- Rules for using email encryption
- Steps for accessing work applications remotely
- Guidelines for creating and safeguarding passwords
- Rules on use of social media

Dark Web: The dark web is the part of the Internet that allows its users to remain anonymous. It is not easily accessible. The dark web facilitates illegal activity such as child sexual abuse, identity theft, drug and firearm trafficking and the planning of terror attacks.

Encryption is the process of scrambling or enciphering data so it can be read only by someone with the means to return it to its original state. Encryption keeps criminals and spies from stealing information. Encryption technologies enable Internet users to protect the confidentiality of their data and communications from unwanted observation and intrusion. Electronic encryption is the process of scrambling or enciphering data so it can be read only by the person who has the key to unscramble it. Modern encryption scrambles data using a secret value or key known only by the recipient and the sender. For stored data, the secret value typically is known only by the data owner. For data communicated over a network, the key is typically known by both the sender and receiver, while for stored data, only the owner knows the key.

End-to-end encryption is any form of encryption in which only the sender and intended recipient can read the message. No third party, even the party providing the communication service, has knowledge of the encryption key. End-to-end encryption is the most secure form of encryption that you can use. So where possible, always use end-to-end encryption to protect yourself and your data. Examples of end-to-end encryption communication services include WhatsApp, Signal, Telegram, and Threema.

Encryption protect your data from being exposed, it also helps:

- Protect data (documents, files, etc.) from tampering;
- Enables trust and security in communications with others;
- Sign digital documents.

Effective encryption is key to secure online communications for everything, from financial transactions to healthcare. It is a foundational component upon which a trustworthy Internet is built. Encryption has a big impact on the global economy, and your daily life. Companies use encryption to protect their sensitive information, like customer information, trade secrets, and financial records. Critical infrastructure, like power plants, use encryption to protect their systems and keep your lights running. Automated teller machines, or ATMs, use encryption to protect your financial information from criminals.

Encryption should be the norm for all Internet traffic. Designers and developers of digital products and services are strongly encouraged to ensure that users' data, whether stored or communicated, are encrypted by default. End-to-end encryption solutions should be made available to all wherever

possible. Network and service operators are encouraged to deploy encryption and firewall policy administrators are urged to allow encrypted traffic.

Data security focuses on protecting data from malicious attacks and the exploitation of stolen data for profit. Ensuring the confidentiality of data provided by individuals and organisations is extremely important and essential in ensuring that all have confidence and trust in the Government's handling of their confidential and personal data. Develop data privacy principles to ensure the protection of the data the government is collecting. Data protection policies and legislation, which will follow this policy, are additional and separate policies and legislation that will ensure citizen data is protected both by Governments, the private sector and any other groups that uses data.

2.0 Global Trends and Approaches

Cyber security threats are increasing. Nation states and state-sponsored actors and criminals are exploiting all PNG citizens by accessing sensitive information and for financial gain. Criminals are using the dark web to buy and sell stolen identities, illicit commodities, and child exploitation material, as well as to commit other crimes. Cyber criminals want to take advantage of the fact that more PNG citizens are more connected than ever before.

Cyber security is at the heart of the transformation to a digital society. As stated in the Digital Transformation Policy, cyber security is a key pillar in ensuring a trusted and secure digital economy. It provides confidence to all citizens and allows businesses to prosper and thrive. The rapid and widespread uptake of digital technology by households and businesses during the COVID-19 pandemic underscores the importance of digital technology as an economic enabler.

To maximise the benefits of digital transformation, PNG citizens must both understand and address the threats that lack of good cyber hygiene brings. Malicious cyber activity is one of the most significant threats impacting PNG and the world around us. The COVID-19 pandemic highlighted the evolving nature of cyber threats. Opportunistic cyber criminals quickly adapted their methods to take advantage of more PNG citizens working, studying and connecting online. Many of them did not have adequate protection because they were just not aware of the danger that lurked at every corner of the online world.

Social engineering and phishing remain an effective threat to enable other types of cybercrime. Criminals use innovative methods to increase the volume and sophistication of their attacks, and inexperienced cybercriminals can carry out phishing campaigns more easily through crime as-a-service. Criminals quickly exploited the pandemic to attack vulnerable people; phishing, online scams and the spread of fake news became an ideal strategy for cybercriminals seeking to sell items they claim will prevent or cure COVID-19.

Nation states and state-sponsored actors seek to compromise networks to obtain economic, policy, legal, defence and security information for their own advantage. Nation states and state-sponsored actors also seek to achieve disruptive or destructive effects against their targets. These actors tend to be sophisticated, well-resourced and patient adversaries, whose actions could impact PNG's national security and economic prosperity. Highly sophisticated nation states and state-sponsored actors continue to target governments and critical infrastructure providers. It is not uncommon for more than 30% of these incidents to try and directly attack a nation's critical infrastructure providers that deliver essential services including healthcare, education, banking, water, communications, transport and energy.

The use of anonymising technologies has made it easier to commit serious crimes at volume and across jurisdictions. It allows criminals and other malicious actors to operate outside the visibility of law enforcement. If our law enforcement agencies are to remain effective in reducing cyber-crime, their ability to tackle the volume and anonymity enabled by the dark web and encryption technologies must be enhanced. As part of this Strategy, the Australian Government will work to ensure law enforcement has the powers and capabilities to investigate and disrupt cyber-crime, including on the dark web.

The GoPNG cannot do this alone, they must work closely with its international partners and the best vehicle to engage with its international partners is to work with the more than 65 different countries who are signatories to the Council of Europe's Convention on Cybercrime and its various protocols.

Encryption continues to be a clear feature of an increasing number of services and tools. One of the principal challenges for law enforcement is how to access and gather relevant data for criminal investigations. The value of being able to access data of criminal communication on an encrypted network is perhaps the most effective illustration of how encrypted data can provide law enforcement with crucial leads beyond the area of cybercrime.

With the rise in connectivity comes a significant increase in cybercrime. Ransomware attacks have become more sophisticated, targeting specific organisations in the public and private sector through victim reconnaissance. While the COVID-19 pandemic has triggered an increase in cybercrime, ransomware attacks were targeting the healthcare industry long before the crisis. Moreover, criminals have included another layer to their ransomware attacks by threatening to auction off the comprised data, increasing the pressure on the victims to pay the ransom.

Child exploitation acts have also grown significantly at the peak of the COVID-19 crisis. Offenders keep using a number of ways to hide this horrifying crime, such as P2P networks, social networking platforms and using encrypted communications applications.

Dark web communities and forums are meeting places where participation is structured with affiliation rules to promote individuals based on their contribution to the community, which they do by recording and posting their abuse of children, encouraging others to do the same.

Livestreaming of child abuse continues to increase, becoming even more popular than usual during the COVID-19 crisis when travel restrictions prevented offenders from physically abusing children. In some cases, video chat applications in payment systems are used which becomes one of the key challenges for law enforcement as this material is not recorded.

The GoPNG needs to develop and actively defend the critical infrastructure that all PNG citizens rely on, including:

- Cyber security obligations for owners and operators.
- New ways to investigate and shut down cyber-crime, including on the dark web.
- Stronger defences for Government networks and data.
- Greater collaboration with other international countries to build PNG's cyber skills pipeline.
- Increased situational awareness and improved sharing of threat information.
- Stronger partnerships with industry.
- Advice for small and medium enterprises to increase their cyber resilience.
- Clear guidance for businesses and consumers about securing Internet of Things devices.
- 24/7 cyber security advice hotline for SMEs and families.
- Improved community awareness of cyber security threats.

3.0 PNG Cyber Security Landscape

PNG's domestic information space is vulnerable to the threat of exploitation and manipulation by external interests. The Country's ability to manage and control information inflows and outflows from its jurisdiction is lacking to the extent that it is unable to safeguard official and critical public information. The lack of control has allowed other states with interest in PNG's affairs to become increasingly knowledgeable on what goes on in the country through effective use of superior information and communication technology.

Additionally, there is an increase in other nation's satellite-based eavesdropping technologies and their strategic value and benefits. The GoPNG is concerned with its national security, and its ability to institute appropriate counter measures to secure its jurisdiction and safeguard all sensitive information and communication. Moreover, the Government must ensure all its agencies in the information and communication industry and other security actors are empowered to facilitate for the improved information security of the country.

In August 2020, the Minister of ICT published several NEC Policy notes asking for increased authority and responsibility to counter these significant increases in Cyber security threats. He called for a joint task force with the Department of Community Development to discuss a proposal for a joint effort to address a wide range of challenges pertaining to cyber safety, cyber security, and cybercrime. The outcome of these meetings was the creation of a Joint Cyber Safety Task Force to jointly address operational matters pertaining to the cyber security, cyber safety, and cybercrime. The NEC also created the National Joint Cyber Safety Shared Services (JCS3) which would include the deployment of specific hardware at all Internet gateways, various key public service agencies leading into Papua New Guinea to enable the implementation and enforcement of mandated functions of each of the agencies within the Joint Cyber Safety Technical Working Group. It also established a National Joint Cyber Safety Operation Centre to facilitate the daily operations of the Joint Cyber Safety Taskforce.

In October 2020, a new NEC Policy Submission recommended the establishment of the Joint Cyber Safety Taskforce and its Terms of Reference; and to endorse the DICT as the lead agency to service the Joint Cyber Safety Taskforce by establishing a National Joint Cyber Safety Operations Centre. The Policy submissions also directs the Cyber Safety Interagency Taskforce to take appropriate enforceable regulatory measures within existing legislative frameworks to deploy appropriate technology at the Internet Gateway for the purpose of administering and enforcing mandated duties pertaining to cybersecurity, cybercrime, and cyber safety with an initial priority to protect the domestic cyberspace from cyber threats.

The NEC Policy submission directed the Social Media Taskforce to review and update, where appropriate, the *National Information and Communication Technology Act 2009,* the *Cybercrime Code Act 2016,* the *Classification of Publication (Censorship) Act 1989* and other enabling legislation to deal with harmful online content including the introduction of enabling policy and legislation for Cyber Security, Data Protection/Data Privacy, and Communications Decency. The same note directed the National Department of Education to update the National Education System Curriculum to include Cyber Safety, Cyber Security, and Cybercrime as compulsory topics under the main subject of Information and Communication Technology

Currently, the GoPNG is not a party or a member of any of the related global Cybersecurity organizations such as the Global Commission on the Stability of Cyberspace (GCSC), The Global Forum on Cyber Expertise (GFCE), and the Global Cyber Alliance (GCA) which provide technical assistance in capacity building, shared knowledge and best practices as well new cyber norms related to prevention and awareness raising, along with international

cooperation, and data collection. Other groups provide a place to exchange best practices and expertise on cyber capacity building. case studies, sharing of real-time threat information across sectors, toolkits to help other organizations and Governments better understand the risks and how to protect themselves.

The GCSC is a multistakeholder commission of experts, who have been working on developing cybernorms for international behavior for over a decade. Their aim is to identify successful policies, practices and ideas and multiply these on a global level. The GCSC is charged with developing proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace.

The Global Forum on Cyber Expertise (GFCE) is another global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level. The GFCE works with over 80 members along with partners from NGOs, the tech community and academia GFCE members to develop practical initiatives to build cyber capacity.

The GFCE has published best practices on the following topics

- National Cyber Security Assessments
- National Computer Security Incident Response
- Incident capture and analytics
- Critical Information Infrastructure Protection
- Legal Frameworks
- Law enforcement in cyberspace
- Cyber Security Awareness
- Standards

The Global Cyber Alliance (GCA) is an international, cross-sector effort dedicated to eradicating cyber risk and improving our connected world. They achieve their mission by: Uniting Global Communities. They work to implement solutions that reduce and eradicate cyber risk and make tools freely available to all. Their goal is to help other organizations, Governments, and businesses, (large and small) prevent cyber-crimes and enhance their cyber security by sharing real-time threat info across sectors. They believe that only by close collaboration between organizations and government agencies could we ensure that critical infrastructure of a city and of businesses and citizens is protected.

The GCA created several toolkits to help other organizations and even local Governments better understand the risks and how to protect themselves

- Cyber Toolkit for Small Businesses
- Cyber Toolkit for Elections
- Automated IoT Defense Ecosystem (AIDE)
- DMARC--Domain-based Message Authentication, Reporting and Conformance
- Quad 9
- Tools to help developers using WordPress and Content Management Systems to secure their website
- Smart Cities and IoT--This interconnectivity poses great risks, however, as cybercriminals can hack into devices and penetrate systems remotely, causing potentially catastrophic damage.

4.0 Policy and Legal Framework

Various policies across different social sector agencies have made efforts, from different perspectives, to identify and highlight the need to address cyber safety, cybersecurity, cybercrime, and cyber resiliency However none has clearly defined all of these definitions in one document and offered suggestions on how to ensure the safety of all critical infrastructure, citizens privacy and data held by them and by the Government.

As a result, PNG remains vulnerable to Cyber-based crimes such as internet gambling, pornography, terrorism, money laundering, and luring rape victims, murder plots.

Additionally, as connectivity increases with the landing of the Coral Sea Cable, hacking of computer systems and theft of trade secrets are on the rise and are very real threats. Unauthorised access to network and computer systems to steal confidential files, for political warfare and for financial gains.

4.1 The Digital Transformation Policy has touched on these issues as has the Corporate Plan, the Cybercrime Act of 2016 and early versions of the Cybersecurity Policy, but there has been no single document that has addressed all these issues. The *Papua New Guinea Digital Transformation Policy 2020* identifies Cyber Safety and cyber resilience as one of its key pillars. It also directs work to be done to increase awareness of these critical issues.

The Policy also recommends for Data Protection and Privacy legislation to be put in place and for the creation of cyber standards and guidelines to be established and published.

4.2 The DICT Corporate Plan 2020-2024. A priority objective of the Department of Information and Communications Technology *Corporate Plan 2020-2024* is, "To ensure an effective Digital safety system to protect public interest against cyber space abuse".

Actions under this Priority Object require the Department of Information & Communications to:

a. Support the review and development of the Cyber Security Policy.
b. Establish the Computer Emergency and Incident Response Team.
c. Conduct awareness on cyber-security issues.
d. Develop a cyber-security Communication Plan.
e. Conduct awareness on cyber safety issues.
f. Develop a cyber-safety communication plan.
g. Work with the Department of Justice, State Solicitor's office and Prosecutor's office and other relevant agencies to ensure all are on board for accession to the Council of Europe Convention on Cybercrime, otherwise known as the Budapest Convention.
h. Identify the various regional groups who are providing training and capacity building activities on cybercrime and digital forensic services.[2]
i. Develop Cybercrime Communication Plan.

[2] The Council of Europe's Global Action on Cybercrime Extended (GLACY+), launched in October 2016, is a joint project between the European Union and the Council of Europe financed by the former under the Instrument Contributing to Peace and Stability and has an overall objective of strengthening the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area. The GLACY+ Project implements activities worldwide across three specific objectives, that is (1) Policies and strategies, (2) law enforcement capacities, and (3) criminal justice capacities.

4.3 The Papua New Guinea National Security Policy 2013

Provision of cyber services in PNG to the public service and to the wide community is not uniform and it changes from agency to agency. The lack of standards, the lack of identification of any particular agency to have control and authority, the lack of appropriate legislation within the Government, and the lack of any international protocols that can help out the Government causes lack of coordination and is a threat to society, threat to the trust held by people in their government, a threat to the countries critical infrastructure, a threat to the privacy and security of citizen's data and a threat to national security.

National Government has in the past passed policies to protect our citizens and to enhance information security. But lack of a data protection and data privacy policy, encryption policies and other related legislation, combined with lack of effective cyber policies, and a lack of a campaign to raise awareness and educate the populace have resulted in this lackadaisical attitude to cyber security, cybercrime, cyber safety and cyber resilience. Policy implementation has been hampered by a failure to design, develop, test, roll-out and regularly maintain and improve a national cyber safety, cyber resilience, cyber security and cybercrime system.

Additionally, the Government is hampered by the lack of any international protocols it can call upon to assist it in its battle to fight cybercrime.

The Papua New Guinea *National Security Policy 2013* is an attempt to give policy guidance. It lists 'Cyber-based Threats', and 'National Information Security' as two of the generic threats to PNG's survival.

Cyber-based Threats is listed as a Level Two Threat. Security threats under this category do not mean that they are any less important but require a lower priority ranking. Depending on circumstances any threat in this category can very quickly be moved to Level One ranking.

4.4 The Papua New Guinea National Security Policy Strategic Action Plan 2014-2020

Policy Goal 8 ('Ensure Technological Security') of the *National Security Policy Strategic Action Plan 2014-2020*: Department of Communications & Information (now Department of Information and Communications Technology) to continue to spearhead a 'whole-of-Government approach' to a single National Information Technology Network supporting e-Governance;

4.5 The National Intelligence Organization Act 1984

The PNG National Intelligence Organization by virtue of the *National Intelligence Organization Act 1984* remains the mandated authority that supports the protection of the Government of the day, all citizens and its legitimate investment and development partners against all forms of undesired threats, economic espionage, terrorism, transnational crimes involving money laundering, human trafficking and so forth in the long term.

4.6 The Classification of Publication (Censorship) Act 1989

- The Censorship Board of Papua New Guinea exists to classify the media content that PNG consumes. It either applies age restrictions to that content, or (in the case of certain illegal content) bans it entirely. There was also an attempt at law reform.

- In 2014, the Censorship Office facilitated drafting of the *Classification of Films, Publication and Online Service Bill 2014* to amend the *Classification of Publication (Censorship) Act 1989* to reflect changing circumstances as technology had become part of everyday life.

4.7 The Gaming Control Act 2007

- Legality of online gambling such as www.pngbet.com is an ongoing issue and the National Gaming Control Board may take action under the *Gaming Control Act 2007.*

- Electronic gambling or lottery by a child is also a cybercrime offence under Section 14 of the *Cybercrime Code Act 2016.* A gaming operator may also be held liable.

4.8 The National Information And Communication Technology Act 2009

- Subject to sections 11 and 58 of the *National Information and Communication Technology Act 2009*, the National Information and Communication Technology Authority (NICTA) may vary an individual licence to incorporate government policy in favour of the deployment of security technology solutions at a licensee's Internet Gateway.

4.9 The Lukautim Pikinini Act 2015

- Subject to section 13 of the *Lukautim Pikinini Act 2015*, the Office for Child and Family Services shall consult with the Department of Information and Communications Technology and other bodies recognized by the Act that are capable of assisting in the protection and welfare of children.

4.10 The Cybercrime Code Act 2016

- The *Cybercrime Code Act 2016* creates powers for constitutional law enforcement bodies but not the capability to perform those powers.

- The Royal Papua New Guinea Constabulary or the Public Prosecutor 17ft he17 respective search, production and investigation powers under Part IV 17ft he Act. But both constitutional bodies have not exercised these 17ft he17 o date due to technical incapability.

- The Act also created legal tests for establishing the criminal liability of ICT Service Providers in PNG under Part V 17ft he Act, which legal tests are heavily reliant on a technical capability on the part 17ft he Royal Papua New Guinea Constabulary to access ICT Service Providers' data for assessing evidence for commission of an offence or an omission against the Act that are critical to proving cybercrimes.

4.11 Alternative Legal Arrangements

4.11.1 MOU Between GOA and GoPNG Relating to Cyber Security Cooperation

- In April 2018, PNG and Australia signed a Memorandum of Understanding (MoU) on Cyber Security Cooperation, after a request from then-PNG Prime Minister O'Neill. The MoU runs until 30 June 2022.

- Initial work under the MoU focused on preventing a major cyber security incident during APEC Leaders' Week (AELW), including establishing the National Cyber Security Centre

(NCSC; co-launched during AELW by the Hon. Sam Basil, then-PNG Minister for Communications and Information Technology, and Australia's Minister for Foreign Affairs. Work has since focused on enhancing PNG's cyber security posture.

- The MoU comprises the following four elements:

    a. Developing and enhancing cyber security governance and best practice frameworks.

    b. Protecting key ICT networks to improve threat awareness, cyber resilience and incident response. APEC venues were initially covered. The NCSC is now protecting the networks of National Information and Communications Technology Authority (NICTA), the PNG Integrated Government Information System, and the PNG Department of Health.

    c. Establishing and running the NCSC to monitor the protected networks for threats and provide incident response support. A multi PNG agency-led Steering Committee governs the NCSC's function.

        i. The Steering Committee is led by the Department of Communications, Information and Technology; NICTA; and Office of Security Coordination and Assessments. The Australian Government and WithYouWithMe, the contracted NCSC delivery partner, also sit on the Steering Committee.

    d. Enhancing PNG CERT capacity (CERTs are the "first responders" during a cyber incident) by providing regular training at the NCSC. This also included a later, separate grant to NICTA to equip the PNG CERT with key, foundational equipment.

4.12 *Management Arrangements*

Australia contracted WithYouWithMe from 17 August 2018 to 30 June 2022 (this coincides with the MoU end date) to partner with PNG in delivering the commitments under the MoU.

To support the transition and PNG control of the NCSC, in early 2020 WYWM shared the NCSC Transition Plan with PNG – a comprehensive set of policy, procedures/ processes and other documentation on which the NCSC's operations are based. As at 29 June 2020, WYWM has also developed an initial draft of an NCSC Change Management Plan. WYWM will partner with PNG to ensure familiarity and ongoing updates.

4.13 ICT Policy

The Government of Papua New Guinea (***Government***) has defined key priorities with regard to the development of ICT in its 2008 National Information and Communication Technology Policy (***ICT Policy***). The ICT Policy paved the way for the liberalisation of the industry and caters for increased competition in the telecommunications sector.

The ICT Policy highlights the importance of building confidence and security in our ICT systems[3]. It underlines the need to protect fundamental rights of citizens as well as enables the investigation and prosecution of crimes. In 2014, the Government introduced the National

[3] *National ICT Policy 2008* p.36

Cybercrime Policy (***Cybercrime Policy***) and subsequently in 2016, enacted the ***Cybercrime Code Act* 2016 (*Act*)**.

The ICT Policy is from 2008 and as such needs to be revised and updated for today's digital economy. While the ICT policy mentions cyber security, it does not limit security concerns to Cybercrime. It also highlighted that "*criminal law is only a small part of the cybersecurity framework*"[4]. The Government further elaborated that Government and Private Sector agencies need to cooperate in improving the security of their systems by applying sound security practices, improving and securing the sharing of information, and raising awareness.

As outlined in the ICT Policy, access to information is beneficial but it is important to be mindful that the same technology provides access to illegal and harmful content.

5.0 VISION AND POLICY GOALS

5.1 Enabling Innovation

The Government is committed to enabling innovation, growth and prosperity for all Papua New Guinean through strong cyber security. This is in line with the GoPMG Digital Transformation Policy to help to create a modern, dynamic, 21st Century economy for Papua New Guinea. Through this policy we hope to:

- Promote collaboration, interaction, and participation,
- Promote Innovation and learning,
- Provide an open and transparent government, and
- Provide citizen-centred services, and Knowledge-based industries.

This vision is one where all citizens are empowered and can interact and collaborate with the Government to achieve the following objectives.

- Create a more secure online world
- Build trust in the online world by supporting businesses' cyber resilience, including by sharing threat information, setting clear expectations of roles and strengthening partnerships.
    - Everyone – governments, businesses and the community – has a role to play in creating a more cyber secure
- Protect our most critical systems and essential services from sophisticated threats.
- Provide law enforcement agencies with greater ability to protect PNG Citizens online, just as they do in the physical world, and target criminal activity on the dark web.
- Protect data and networks through a new Data Protection and Data privacy legislation.
- Create a voluntary Code of Practice will set out the GoPNG security expectations for internet-connected consumer devices. The GoPNG will work with industry to consider and clarify the cyber security obligations of industry in the future, including through regulatory reforms.
    - Insist that businesses can only sell products and services that are secure

[4] *Ibid*., p.38 *ff*

- Partner with the private sector, especially large businesses to assist small and medium enterprises (SMEs) to grow and increase their cyber security awareness and capability.
    - Government will work with large businesses and service providers to provide SMEs with cyber security information and tools as part of 'bundles' of secure services (such as threat blocking, antivirus, and cyber security awareness training).
- Expand efforts to raise awareness of cyber security threats and empower the community to practise secure online behaviours.
- Strengthen partnerships with other Pacific Nations and other countries in the war against cyber criminals.

This vision establishes seven themes of action for Papua New Guinea cyber security over the next five years:

- A national cyber partnership
- Strong cyber defences and cyber resilience
- Cross cutting critical infrastructure to focus processes and identifying those that deliver critical services/functions to the nation
- Global responsibility and influence
- Growth and innovation, working with the business community to create a code of conduct for all products and services and work with all businesses to increase their cyber capabilities
- Increasing cyber awareness and education with PNG
- Expand efforts to raise awareness of cyber threats

This vision and strategy can only be successful if everyone works together to build up cyber resilience. Businesses should take responsibility for securing their products and services and protecting their customers from known cyber vulnerabilities. Consumers should take responsibility for practising secure online behaviours and making informed purchasing decisions.

Although PNG has been lucky to avoid a catastrophic cyber security incident, we are vulnerable to the cyber attacks experienced elsewhere in the world. Supporting the continuity of essential services in the face of disruptive or sophisticated attacks is a fundamental obligation for government.

The loss of an essential service like electricity, water or transport could have devastating impacts across all of PNG far beyond the targeted business. There is lots more that can be done to raise the overall security posture of critical infrastructure, some nation states or state-sponsored actors are so sophisticated that an attack may be beyond the capability of a single network owner to handle alone, irrespective of its size, expertise and best efforts.

We will work with our allies and donors to assist us in strengthening our capacity to prevent or respond to malicious cyber activity, including in response to sophisticated actors.

To meet these goals the GoPNG needs to identify the systems across all vital infrastructure sectors within the GoPNG that need to be hardened and also to identify the series of tasks and information exchange that need to be readily secured and replicated as in disaster management and business continuity plans. These include creating string guidelines and policies in ensuring cloud security for critical infrastructure.

It also must create policies, guidelines and standards for cyber security, cyber safety and cyber resilience.

It also must lay out a series of best practices such as:

- Restricting users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services.
  - Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application whitelisting to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

Additionally, all users should follow these precautions to protect themselves against the threat of ransomware:

- Update software and operating systems with the latest patches.
- Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in emails.
- Backup data on a regular basis. Keep it on a separate device and store it offline.
- Follow safe practices when browsing the Internet.

Being connected is now essential, creating new opportunities for innovation and growth for all people in PNG. To be competitive, businesses need to be online. But being online also brings risks. PNG is increasingly becoming a target for cyber intrusions and cybercrime. All of us—governments, businesses and individuals—need to work together to build resilience to cyber security threats and to protect the country's critical resources.

For PNG to grow and become an active member of the connected nations of the world, PNG needs to innovate and further diversify its economy—to access new markets and new forms of wealth creation. We must embrace disruptive technologies; We must open up new possibilities for businesses to grow and develop in ways as yet unimagined.

But the potential of digital technologies depends on the extent to which we can trust the Internet and cyberspace. Getting cyber security right will mean we capture more of the opportunities the connected world offers. It will also make PNG a preferred place to do business. This in turn will boost our national prosperity. We can also expand our cyber security businesses and export capability.

Malicious cyber activity is a security challenge for all people in PNG. Outside of PNG, many nations, including Australian organisations across the public and private sectors have been compromised by state-sponsored or non-state actors. In many countries, cyber criminals have targeted local governments, airports, hospitals and other critical infrastructure crippling governments and putting the health of people at risk. Large multinational companies and government organisations have been targeted, losing substantial amounts of sensitive commercial and personal information or incurring major damage to their business and reputation.

To grow our cyber security capabilities to anticipate and respond to cyber threats, we must address this issue. It is critical that we build our nation's stock of cyber security skills, which are becoming increasingly essential for life and work in our connected world. To respond to these challenges we must elevate cyber security as an issue of national importance. Leadership will be critical to achieving this goal.

The socio-economic development of PNG has become increasingly dependent on the use of ICT services and applications. The Government is therefore committed to ensuring that citizens, visitors, businesses and government agencies enjoy the full benefits of a safe, secure and resilient cyberspace.

5.2 Policy Goals

Cybersecurity threats and threats to GoPNG's critical infrastructure are rapidly increasing and so needs to be factored into any ICT policy. Attacks on its critical systems and essential services and those of the country, can adversely affect national security, economic security, public health, safety, administration, or a combination of all these as we become increasingly reliant on interconnectivity.

As people and systems become increasingly interconnected, the quantity and value of information held online has increased. So have efforts to steal and exploit that information. Cyberspace, and the dynamic opportunities it offers, is under persistent threat. Malicious cyber activity is a security challenge for all citizens of PNG. Worldwide, losses from cyber security attacks are estimated to cost economies around one per cent of GDP per year.

Cyber adversaries are aggressive and persistent in their efforts to compromise PNG networks and information. They are constantly improving their tactics to infiltrate government, private sector and other networks. They will also target the weakest link; if the network security of their primary target is robust, they will move to more easily compromised connected networks that could provide access to the primary target.

Furthermore, the differences between some malicious cyber actors—such as organised criminal networks, state-sponsored actors and issue motivated groups—are becoming less and less distinct. For example, activity by some cyber criminals can be more sophisticated than those conducted by many nation states. This growing network of malicious actors is having a global impact. Malicious cyber activities are wide ranging. They include activities designed to compromise the confidentiality, integrity or availability of computer networks or ICT systems or the information on them.

In this policy cyber attacks refers to deliberate acts that **seriously** compromise national security, stability or prosperity by manipulating, denying access to, degrading or destroying computers or networks or the information resident on them. Other compromises are referred to as 'malicious cyber activity'.

The Government recognises that the lack of a coordinative Cybersecurity institution or agency only adds to these risks, as such, it has established the National Cybersecurity Centre (***NCSC***), and commends the establishment of PNGCERT through the Public Private Partnership (***PPP***) arrangement. In addition, it acknowledges the requirement of a national and or government CIRT. The recently established CSOC under the proposed NCSC will therefore be a fundamental priority and focus of this Policy.

A coordinated approach led by the Government is a key step towards Cybersecurity preparedness and resilience to counter cyber threats and attacks. In this vein, common standards and practices on Cybersecurity within Government, and guidelines to businesses need to be created. Appropriate and relevant legal and regulatory frameworks are also required to define and support common standards, practices and guidelines. Capable institutions with adequate capacity are also essential to lead and enhance Cybersecurity activities.

National co-leadership and cross-sectoral partnerships are essential for strong cyber security. As stated, cyber security needs to be driven from the top. Economic and national security imperatives mean that cyber security is a strategic issue for leaders—Ministers, senior executives and boards—not just for ICT and security staff.

There is a great need to have more collaboration with the private sector, the technical community and governments. These discussions need to focus on practical outcomes and elevate cyber security, both as a business risk and as a strategic opportunity rather than just as an operational matter.

Government and business leaders can do more to raise cyber security's prominence within their organisations, teams and peer groups. Including cyber security as a priority for corporate boards and international leaders will demonstrate that cyber security is a strategic priority for PNG.

We can start by conducting a cyber assessment within both the Government, educational institutions and other organizations. Based on the result of this assessment the GoPNG can better understand the level of knowledge of cyber safety within the country and then implement a training and awareness plan to overcome these deficits.

Governments, universities, civil society, and firms large and small in the private sector need to better understand cyber risk. Strengthened cyber security partnerships across the public and private sectors will give us a competitive advantage and increase PNG's potential as a modern, connected and innovative economy.

Under this Policy, Government, civil society, the technical community and business all need to work together to design a national cyber security strategy and standards. The meetings will bring together leaders from many sectors of the PNG economy to discuss how Government, civil society, and business can collaborate to strengthen our economy and national security by building greater resilience to cyber security threats.

Organisations need easy and consistent interfaces with Government agencies on cyber security. A new streamlined Government cyber security structure will bring together disparate elements of both the policy and operational areas.

The GoPNG will work with the Ministry of Education and the National Research Institute to create a curriculum to introduce Cyber security and cyber safety into the elementary, high schools and universities enabling a smarter and safer workforce.

The following goals are aimed at fostering a coordinated approach led by the Government to ensure Cybersecurity preparedness and resilience through:

- Developing and strengthening legal and regulatory frameworks consistent with the highest regional and international standards in the larger field of Cybersecurity,

incorporating legislation on the protection of critical infrastructure, privacy and data protection, information sharing, e-Commerce, freedom of information or access to information, and child online protection and to enhance Cybersecurity of persons with disabilities; to complement the existing ***Cybercrime Code Act*** **2016**, while maintaining a balance between individual and collective security and preserving the right to privacy and other fundamental rights and freedoms of citizens;

- Creating institutional capacities and strengthening existing structures as Cybersecurity coordinative institutions;

- Developing and implementing technical measures, appropriate frameworks, standards and guidelines and enabling capacity to protect critical infrastructure systems and services against cyberattacks;

- Providing businesses and citizens with access to basic services and actionable intelligence related to Cybersecurity;

- Creating and increasing knowledge and awareness of Cybersecurity and ways to protect against cyber threats to Government, businesses and citizens, and providing basic tools and services as well as expertise to the highest standards;

- Creating a secure ICT environment that enables constant exchange of information amongst stakeholders;

- Strengthening the country's ability to participate in international cooperation arrangements in order to harness the global nature of Cybersecurity challenges, and

- Implementing protective technical measures aimed at reducing online threats and create a safe cyber environment for children.

This national Cybersecurity Strategy will outline action plans towards implementing the goals set out in this policy. This Strategy will harmonise differing standards and practices in order to strengthen and enhance Cybersecurity within Government and provide guidance to businesses and the country as a whole. The Strategy will take into account national demands as well as international best practices, and will be kept in the custody of the Prime Minister's Office as head of the NSC under the auspices of the National Security Advisory Committee (***NSAC***).

The implementation of the Digital Transformation Policy, the forthcoming Data Protection/Data Privacy Policy, Cloud Policy and other related polices along with a revised Universal Access policy will have a major impact on ensuring that all PNG citizens can gain access to meaningful connectivity within the country, particularly in remote and rural areas. However, with this increased connectivity PNG has become a target rich environment for cyber criminals to hijack and cause havoc for all citizens. It is why it is so imperative that the PNG Government create a series of standards and Guidelines as well as dramatically increase awareness of proper cyber safety and cyber hygiene for all citizens. It is also why the ICT Minister along with the Religion, Youth, and Community Development has issued an NEC Policy Submission and the Government has created the Joint Cyber Safety Task Force to directly address these issues.

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and

nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services.

However, Cyberspace is difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an very high priority for the GoPNG.

Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment. Every time we connect to the Internet—at home, at school, at work, or on our mobile devices—we make decisions that affect our cybersecurity. Emerging cyber threats require increased engagement from the entire PNG community to create a safer cyber environment—from government and law enforcement to the private sector and, most importantly, members of the public.

There is a great need to create a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering all PNG citizens to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

We need to engage, educate, and work with our public, private sector partners along with our partners in Civil Society and the Technical Community through events and initiatives with the goal of raising awareness about cybersecurity and increasing the resiliency of the nation in the event of a cyber incident. Within the Pacific region many countries conduct several awareness campaigns and host other Cyber Security Awareness activities throughout to increase the awareness and educate the populace, government workers and all people. It is only by everyone working together that we can keep everyone safe. Cybersecurity and keeping the Internet safe for everyone is a shared responsibility.

It is hoped that the Joint Cyber Safety Task Force can coordinate with sector specific agencies, other federal agencies, and private sector partners to share information on and analysis of cyber threats and vulnerabilities and to understand more fully the interdependency of infrastructure systems nationwide. To work with work with other agencies so that it can employ a risk-informed approach to safeguarding the government's critical infrastructure in cyberspace.

This collective approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents prioritizes understanding and meeting the needs of our partners, and is consistent with the growing recognition among corporate leaders that cyber and physical security are interdependent and must be core aspects of their risk management strategies.

The JCSF will work to emphasize protections for privacy and civil liberties, transparent and accessible security processes, and domestic and international partnerships that further

collective action. The JCSF coordinates with sector specific agencies, other government agencies, private sector partners along with the Technical Community to share information on and analysis of cyber threats and vulnerabilities and to understand more fully the interdependency of infrastructure systems nationwide. This collective approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents prioritizes understanding and meeting the needs of our partners, and is consistent with the growing recognition among corporate leaders that cyber and physical security are interdependent and must be core aspects of their risk management strategies.

The National Cyber Security Centre (NCSC)'s mission is to reduce the risk of systemic cybersecurity and communications challenges in our role as the GoPNG flagship cyber defense, incident response, and operational integration centre. Since 2018, the NCSC has served as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating out 24/7 situational awareness, analysis, and incident response centre.

The National Cyber Security Centre (NCSC) conducts defensive cyber security operations by:

- conducting audits on endpoint cyber security tracking and monitoring systems used by public bodies and digital services;
- recommending to the Head of Department and all other relevant authorities the prosecution of cyber offences under this Act and all other relevant laws;
- facilitating and promotes a secured digital government environment
- protecting classified and sensitive government information.
- Maintainung the critical infrastructure that contains security control technologies for NCSC and its constituents;
- Monitoring and investigates threats across network and endpoints;
- Providing technical support to the Papua New Guinea Computer Emergency Response Team (PNGCERT)
- Documenting NCSC's Operational Process and provide guidelines to solving incidents;
- Mitigating or resolving a computer security incident.
- Ensuring that threats attacking data and assets are contained and eliminated;
- Handling incidents in the event of a breach, investigate the source and escalating to higher authorities where necessary for their interventions;
- Providing a process so that its customers and other member organizations of PNGCERT can report cyber-attacks or suspected cyber incidents to NCSC;
- Training staffs on the operational process, incident management and handling, ICT infrastructure and technology handling and new emerging technologies;
- Providing its constituents with remote incident response and handling support;
- Gathering and storing forensic artifacts, e.g., flash-drives, hard-drives and all others related to an incident, in a manner that enables admission of evidence in a legal proceeding;
- Monitoring operational security controls;
- Providing technical advice on cyber security program management;
- Ensuring on-going delivery of technical training and development of public body officials for cyber security and related purposes.

This is consistent with the government endorsed *ICT Sector Roadmap 2018*[5] which identified "cyber safety*"* as one of its main pillars.

[5] The *ICT Sector Roadmap 2018*, endorsed through NEC Decision No. 289/2018

A key step in developing a thriving ICT ecosystem is to provide PNG consumers and businesses with the confidence they need to undertake transactions online. It is here where the DICT works closely with all agencies to assist them in improving their cyber hygiene, increase their awareness of cyber threats, and provide resources to help agencies ensure that critical infrastructure and services are protected.

Tools to prevent fraud and promote trust should be developed and provided to consumers and businesses. Mutual trust is the key to interactions in which the government collects information about citizens and citizens provide their own data to the government. Without trust, users feel vulnerable and marginalized and are reluctant to take advantage of the many legitimate benefits that the Internet offers.

Trust is a key ingredient for a sustainable, evolving and global Internet. It is the cornerstone for all successful connectivity strategies. An 'open and trusted Internet' is a globally interoperable Internet that cultivates innovation and creates opportunities for all. Its foundation lies in user trust, technologies for trust, trusted networks and trustworthy ecosystems.

Building user trust means putting in place the right infrastructure (trusted networks), empowering users to protect their activities (technologies for trust), setting the right policies, and providing a responsive environment that properly addresses users' well-founded concerns (trustworthy ecosystem).

Equally important is ensuring the cyber security of all critical ICT infrastructure in PNG and preventing cyber-attacks; this will help to create a stable environment and promote the use of digital services. Finally, the development of legislation on consumer rights, data privacy, and data protection can help give consumers confidence to trust online services. The point is technology alone cannot ensure the privacy of personal data. Most privacy protection protocols are still vulnerable to authorized individuals who might access the data.

Data protection and data privacy laws, which will follow this policy, are legislation enacted to protect personal, commercial, and governmental data from unauthorized access, alteration (corruption), destruction, or use and prevent a host of cyber .

5.3 Importance of Ensuring Cyber Resilience of Critical National Infrastructure

While cyber security is foundational to protecting assets from an attack happening in the first place. Cyber resiliency concerns the assurances for a nation that its critical infrastructures will remain effective and operational for it to endure inevitable attacks.

Attribution of responsible attackers is a capability enabled by threat intelligence analysis of multiple sources of information to learn tactics, techniques, and procedures used by attackers. This information enhances methods for security and resiliency. Transparency of these capabilities, propensity for risk, and cultures are challenges to national cyber strategies being comparable to protect our tightly woven digital economies

5.4 Policy Principles

The Policy will therefore be guided by the following principles:

- Protecting citizens, visitors, businesses and government agencies and critical infrastructure by providing the necessary security frameworks, strategies and guidelines, building national capacity, implementing information sharing techniques and raising awareness;

- Engaging all stakeholders nationally and internationally, in the implementation of this Policy consistent with the Public-Private Partnership policies of the Government;

- Ensuring timely implementation of this Policy so that Cybersecurity measures are implemented commensurate with the increase in services and connectivity and the country's emerging prominence within the region;

- According equal attention to strengthening existing child protection legislation and introducing or adopting technical measures for Child Online Protection, and enacting legislation in areas such as privacy and data protection, critical infrastructure protection and e-Commerce;

- Ensuring appropriate legislation and regulations focusing on technical minimum standards to support the implementation of this Policy; and

- Taking into account in the implementation of this Policy, relevant national, regional and global best practices in building confidence and security in ICT by cultivating strong linkages with the different UN organizations and international organizations working in this arena..

6.0 ROLE OF GOVERNMENT IN CYBERSECURITY

The Government plays a significant role in the protection and enhancement of Cybersecurity in the country. The Prime Minister and the Cabinet need to take a leading role in the protection, enhancement, and strengthening cyber resiliency of PNG critical national infrastructures. The Government will strengthen its current lead role on cyber security policy and be the central point for policy issues to ensure a simplified Government policy interface for stakeholders. This Department will provide integrated oversight of the Government's cyber security policy and implementation of this Strategy. It will also prioritise the Government's activities against the Strategy's national cyber security objectives.

The responsibility to secure Government Information systems and national security systems — falls squarely on the Government of PNG. The Administration will clarify the relevant authorities, responsibility and accountability within and across departments and agencies for securing Government information systems, while setting the standard for effective cybersecurity risk management.

The Government will clarify the roles and responsibilities of government agencies and the expectations on the private sector related to cybersecurity risk management and incident response. Clarity will enable proactive risk management that comprehensively addresses threats, vulnerabilities, and consequences. It will also identify and bridge existing gaps in responsibilities and coordination among government and non-government incident response efforts and promote more routine training, exercises, and coordination.

The GoPNG Enterprise Architecture depends on information technology (IT) systems and computer networks for essential operations. These systems face large and diverse cyber threats that range from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems.

Many public service agencies, responsible for official government information and services, are already using public cloud-based infrastructure and services, driven by business requirement cost efficiencies, ahead of government policies, standards, and guidelines, maybe exposing government and citizens data to malicious 3rd party intermediaries unknowingly, with or without citizens' concerns and understanding of the exposure and associated risks that may be outside government jurisdiction to administer or intervene in event of any breach.

The cloud platform provides access to many powerful tools and services such as big data analysis, artificial intelligence, that be very useful for intended purposes or can be disruptive against standing government constitutional boundaries, policies, including data protection and privacy if such government and personal data fall in wrong hands in the cloud environment.

The COVID-19 crisis has revealed how governments without coordinated mature information governance, data protection, and privacy mechanism are being preyed on by criminals, a threat landscape that is always existing and is recently manifested by the COVID-19 crisis, and also through citizens and business increase use of digital services.

The Government will work with the private sector to manage risks to critical infrastructure at the greatest risk. The Government will develop a comprehensive understanding of national risk by identifying national critical functions and will mature our cybersecurity offerings and engagements to better manage those national risks. The Government will prioritize risk-reduction activities across critical key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation.

ICT providers within PNG are in a unique position to help the GoPNG to detect, prevent, and mitigate risk before it impacts customers, and the Government will work with each of these providers to improve ICT security and resilience in a targeted and efficient manner while protecting privacy and civil liberties. The Government will work to strengthen our efforts to share information with ICT providers to enable them to respond to and remediate known malicious cyber activity at the network level.

The Government will continue to encourage reporting of intrusions and theft of data by all victims, especially critical infrastructure partners. The prompt reporting of cyber incidents to the Government is essential to an effective response and prevention of future incidents.

Cloud security is now essential in any new cyber policy[6]. Cloud Security involves the procedures and technology that secure cloud computing environments against both external and insider cybersecurity threats. Cloud security and security management best practices designed to prevent unauthorized access are required to keep data and applications in the cloud secure from current and emerging cybersecurity threats.

[6] Cloud computing, which is the delivery of information technology services over the internet, has become a must for businesses and governments seeking to accelerate innovation and collaboration.

The Government will work to update electronic surveillance and computer crime statutes to enhance law enforcement's capabilities to lawfully gather necessary evidence of criminal activity, disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious cyber actors.

Cloud security differs based on the category of cloud computing being used. There are four main categories of cloud computing:

- **Public cloud services, operated by a public cloud provider** — These include software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).
- **Private cloud services, operated by a public cloud provider** — These services provide a computing environment dedicated to one customer, operated by a third party.
- **Private cloud services, operated by internal staff** — These services are an evolution of the traditional data center, where internal staff operates a virtual environment they control.
- **Hybrid cloud services** — Private and public cloud computing configurations can be combined, hosting workloads and data based on optimizing factors such as cost, security, operations and access. Operation will involve internal staff, and optionally the public cloud provider.

Understanding your security responsibility is the first step to building a cloud security strategy. The GoPNG as noted in its NEC Policy Submission on Public Sector Cloud Services, plans to use a hybrid infrastructure which is composed of a combination of on-premises data centers, private clouds, and/or public clouds where enterprise systems and applications can be deployed on these platforms based on different business requirements. The hybrid cloud infrastructure from an industry perspective is too compelling for the government to ignore. By adopting a hybrid approach, government organizations can overcome the security and data sovereignty issues of the past to deliver a new generation of cost-effective and innovative citizen services

The Joint Cyber Security Task Force works with each Ministry, Agency or department to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever-changing threats. As systems are protected, alerts can be issued at machine speed when events are detected to help protect networks across the government information technology enterprise and the private sector. This enterprise approach will help transform the way federal civilian agencies manage cyber networks through strategically sourced tools and services that enhance the speed and cost effectiveness of federal cybersecurity procurements and allow consistent application of best practices.

The adoption by the GoPNG of a Private Secure Data Exchange platform to connect the various Government data infrastructure will help to promote security within the Government network. It is just critical and essential that these platforms fall under the GoPNG's critical infrastructure.

The JCSTF will work with its partners to provide GoPNG Agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant

problems first. It is their goal to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources.

The JCSTF role is also to protect the critical infrastructure within the Government. Its job is to ensure that the Government has the correct Cyber resiliency standards and guidelines that are needed to ensure that all infrastructure and essential services are protected from attack.

Critical infrastructure top targets are:

- Public/government
- Telecommunications
- Health
- Academic
- Manufacturing
- Power/utility, and
- transportation
- General information warfare threats

Protection at all times, but especially at times when a Government's defenses are down during pandemics, are prime time for criminals to attack. Criminals are using innovative methods to increase the volume and sophistication of their attacks, and inexperienced cybercriminals can carry out phishing campaigns more easily through crime as-a-service. Criminals quickly exploited the pandemic to attack vulnerable people; phishing, online scams and the spread of fake news became an ideal strategy for cybercriminals. This is some of the work that the JCSTF will do in protecting the country.

Leadership and advocacy of this work will be driven by a new position in the Prime Minister's office. This Special Adviser will lead the development of cyber security strategy and policy, provide clear objectives and priorities to operational agencies and oversee agencies' implementation of those priorities. The Special Adviser will also ensure the Government is partnering effectively with other agencies and with provisional and local level governments, the private sector, civil society, the technical community, academia, and international partners.

There is a great need to gather better statistical data on the national impact of cyber security compromises will enable PNG businesses and governments to make informed decisions when managing cyber risks. Data collection measures will help the GoPNG and the private sector to better make decisions that address cyber security threats to PNG's economy and security.

To better help PNG citizens the Government will:

- Assume the lead role in coordinating nationally and internationally, efforts in addressing Cybersecurity threats;
- Initiate the development of necessary frameworks;
- Provide necessary resources including, funding, CIRTs, human resource training and capacity building, and necessary hardware and software infrastructure, to counter cyber threats;
- Identify from time to time, and protect critical government assets and systems including the Integrated Government Information System (***IGIS***), NICTA's Automated Spectrum Management System (***ASMS***), Integrated Financial Management System (***IFMS***), NID System and other functions which are dependent upon or functional on electronic systems;

- Raise awareness and education;
- Initiate and facilitate activities to protect and enhance Cybersecurity in the country.

Deterring cybercrime requires a credible threat that perpetrators will be identified, apprehended, and brought to justice. In this vein, we will work with other parts of the Government to accede to the Council of Europe's Convention on Cybercrime so that we can gain the immediate cooperation of all members to combat cybercrime and catch the perpetuators.

7.0 KEY ISSUES AND CHALLENGES

Today, economic security of PNG is inherently tied to the country's national security. As the foundations of our economy are becoming increasingly rooted in digital technologies, the GoPNG will model and promote best practices and standards that protect our economic security and reinforce the vitality of all citizens.

Governments have a responsibility to lead by example. Moving more government services online will make the lives of many PNG citizens easier, however, citizens need to have confidence that their data is safe, underscoring the need for government systems and data to be secure. This Strategy combined with the Digital Transformation Policy, the Digital Government Act and future legislation such as Data Protection/Privacy and Communications Decency will strengthen the defences of PNG's public sector networks.

The GoPNG will work collaboratively across all stakeholder groups, from the private sector and civil society, to the academic and technical community to promote best practices and develop strategies to overcome market barriers to the adoption of secure technologies. The Government will improve awareness and transparency of cybersecurity practices to build market demand for more secure products and services. The GoPNG will collaborate with international partners to promote open, industry-driven standards and risk-based approaches to address cybersecurity challenges to include cloud security, platform and managed service approaches that lower barriers to secure practice adoption across the breadth of the ecosystem.

Internet security requires a combination of several products and technologies to properly safeguard data. It's important to consider several types of internet security strategies when taking proper measures to help keep your network secure. These tactics can include:

- **Browser selection:** Each browser has its own security measures in place, but some can have serious flaws that allow hackers and cybercriminals to exploit and invade. Ensure that you're using a secure browser to reduce the risk of compromising your computer or network.
- **Multi-factor authentication (MFA):** MFA is a method of controlling computer access by requiring several separate pieces of evidence to an authentication mechanism. Websites and email accounts can be made more secure by requiring at least two factors of authentication by a user.
- **Email security:** Email creates a wave of opportunity for viruses, worms, Trojans, and other unwanted programs. Establishing a multi-layered and comprehensive email security strategy will help significantly reduce exposure to emerging threats. Email messages can also be protected by using cryptography, such as signing an email, encrypting the body of an email message, and encrypting the communication between mail servers.

- **Firewalls:** Firewalls act as filters that protect devices by allowing or denying access to a network. By applying a specific set of rules to identify if something is safe or harmful, firewalls can prevent sensitive information from being stolen and keep malevolent code from being embedded onto networks.

This Policy ensures a collaborative and coordinated approach towards effectively addressing the national Cybersecurity agenda. Cyber threats and attacks are rapidly evolving in form and level of sophistication. It is therefore important to ensure that people and businesses in PNG have access to regularly updated information about threats and vulnerabilities as well as best practices to manage and mitigate risks and prevent attacks.

Government will address the challenges by creating institutional capacities within the country to monitor developments and provide related services, guidance and information which, will be entrusted to respond to Cybersecurity threats and or incidents to raise awareness, disseminate information and provide relevant services for citizens, businesses and Government.

Government recognizes the global challenge of cyber threats. Cyber threats are everywhere. We cannot close our borders and hope we will not be infected. Cyber threats are not just an international phenomena but a global one.

Governments, whether in developing or highly developed countries, need the cooperation of all stakeholders to protect the country and themselves against cyber-attacks.

The prevention of attacks, the detection of illegal activities as well as the recovery from breaches to Cybersecurity, require skilled experts. Currently, there are very few such experts in PNG and the demand for relevant expertise in both the private and public sectors is increasing. PNG will address the challenge by introducing and supporting programs to create and strengthen expertise within the country.

To respond to trends and new developments, the Government and the specialized institutions require up-to-date information about attacks both within the country and globally. PNG will address the challenges by developing a bi-directional reporting mechanism including, information sharing which is fundamental to effective Cybersecurity.

To better detect, deter and respond to malicious cyber activities, cyber threat information should be shared in real time between and within PNG's public and private sectors. Both have unique information to contribute to the threat picture. It is only by combining our knowledge that we can comprehensively understand cyber security threats to Australia and how to counter them. It is equally important to deter malicious cyber activities by better understanding the threat and bringing the perpetrators to justice.

Strong cyber security ensures organisations can better detect malicious cyber activity. It can also be an effective deterrent by increasing the effort necessary for an attacker to succeed. Further, it can ensure that when malicious activity does occur, the consequences are reduced and the extent of the activity is contained effectively.

Many PNG consumers and organisations are also simply unaware of the risks they face in cyberspace. Businesses own and operate most of the infrastructure in cyberspace. They have information about malicious cyber activities on their networks and systems that is not readily available to Government agencies. At the same time, Government has access to intelligence and other restricted information about cyber security threats that is not readily

available to businesses. There needs to be increased cooperation and collaboration between both groups.

While detecting and responding to cyber intrusions is important, even more important is to harden our networks and systems and make them less vulnerable to intrusions. In this case, prevention is definitely better than the cure.

All Stakeholders must work together to build a collective understanding of cyber threats and risks through a layered approach to cyber threat sharing. By securely sharing sensitive information and working together we can better fight against cyber intrusions and cyber threats. This collaboration includes identification and detection of patterns of malicious cyber activity and implementing adaptive and behavioural analysis to enable an epidemiological approach to responding to cyber threats.

Pooling our resources is more efficient and will help develop quicker responses to compromises and build national resilience. We can draw from the positive lessons learned from other successful cyber security partnerships, such as the current partnership with Australia on Cybersecurity.

A strong workforce of skilled cyber security professionals is a key enabler for the growth of digital economy and security. The Government will work with the private sector and the ICT community to enhance awareness and knowledge of cyber security and of proper cyber hygiene. The Government will work with all Ministries including the Ministry of Education and the Ministry of Higher education to create a curriculum that can teach our students cyber skills so that we can grow and create a cadre of skilled cyber security professionals within PNG for the future. Growing the cyber security skills pipeline will ensure all critical infrastructure owners and operators and businesses have greater access to skilled cyber security professionals with the right skills to meet demand.

The PNG Government is committed to equipping all consumers with the right cyber security skills and raising levels of cyber security awareness so we can all benefit from the opportunities in cyberspace. A Cybersecurity policy is vital as it provides a clear direction for the Government to deal with issues of Cybersecurity.

Both government and businesses have finite resources. The actions outlined in this policy and strategy address the most urgent issues. Technology is constantly changing; measures designed to improve security in today's online world can be quickly overtaken by new technologies, systems, software and applications.

8.0 Cybersecurity Education and Awareness Campaign

This is the training and awareness part of the strategy to make all PNG citizens aware of the need for proper cyber hygiene and protection.

It could be modelled after the Australian e-Safety Commission. I would envision that modules could be created on each of these areas and there could be posters similar to what the Health department did for Covid.

- Training of Agency personnel on Safe Cybersecurity practices
- Adapting training material from Global Cyberspace Agenda and other related cyber groups to the PNG marketplace

- Creation of posters, social media and other tools to raise awareness of proper cyber Hygiene
- Translating some of the cyber courses on various platforms such as ICANN Learn, ISOC Learn, APNIC and other platforms to the PNG Marketplace
- Hosting a series of cyber webinars in conjunctions with PICISOC, PNG ICT Cluster, Technical Community such as APNIC, ISPs, ICANN, etc
- Provide online safety and guidance
- Provide educational resources and training on online safety
- Introduction of cyber security and proper cyber hygiene in University and into the curriculum
- Introduction of cyber security and proper cyber hygiene in elementary and in high school and working with the Department of Education to add it to the curriculum