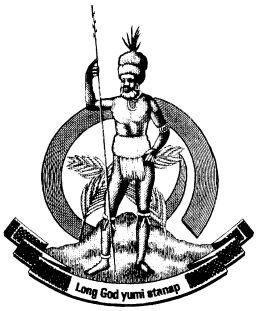
Republic of / République de / Ripablik blong Vanuatu

National Cybersecurity Policy

Politique nationale de cybersécurité

Nasonal Cybersekuriti Polisi

DECEMBER / DECEMBRE / DISEMBA 2013



Republic of / République de / Ripablik blong Vanuatu

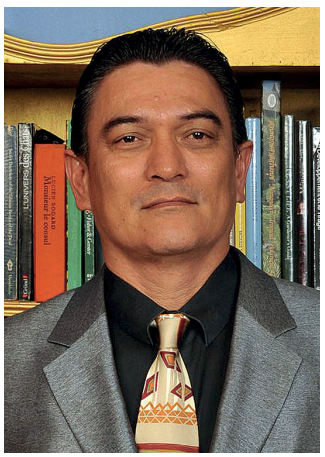
National Cybersecurity Policy

Politique nationale de cybersécurité

Nasonal Cybersekuriti Polisi

DECEMBER / DECEMBRE / DISEMBA 2013

Foreword



Hon. Moana Carcasses Katokai Kalosil, Prime Minister of Vanuatu

I have the pleasure to present to you this Cybersecurity Policy. This Policy expresses a firm commitment of the Government to maximise the safety and security of information and communication technologies in achieving the National Vision of "A Just, Educated, Healthy and Wealthy Vanuatu", thereby empowering and benefiting every citizen and resident of Vanuatu.

This Government's commitment will first of all be expressed through goals set out in this policy to ensure citizens of Vanuatu, tourists, businesses and government enjoy the full benefits of a safe, secure and resilient cyber space enabling them to get access to knowledge and share information while understanding and addressing the risks, to reduce the benefits to criminals. The Policy unleashes creative collaboration and action between the private sector and the government for joint coordination and collaboration to achieve the goals of this policy.

The arrival of the Interchange Submarine Cable project will provide a high-speed reliable link for Vanuatu to the World. This means internet users at large are exposed to risks experienced by other countries. Sector institutions, specifically the multi-stakeholder Cybersecurity Working Group, the Office of the Government Chief Information Officer, the Telecommunications and Radiocommunications Regulator, Internet Service Providers (ISPs) are tasked with a challenging role to ensure Vanuatu is resilient to such cyber attacks .

In our work we have enjoyed support of our friends in a multitude of international and regional organisations, as well as our development partners. I would like to express a special thanks to the International Telecommunications Union (ITU), which has consistently supported the institutional and policy development in the Cybersecurity area in Vanuatu, through the ICB4PAC program for the Pacific Islands which Vanuatu is a beneficiary.

A lot has been achieved. However, a lot is yet to be done. ICTs have a strong potential to transform education of our children, expand and improve government services, make us more resilient in the face of natural disasters, preserve and promote our culture, as well as provide new business opportunities, and generally enhance our livelihoods. They will bring us closer together and strengthen our connection to the World. However, actual benefits depend on all of us working together — the Government, private sector, academia, users, civil society, and, ultimately, every citizen and resident. Only together can we transform this potential into reality that we will feel every day.

I am calling on all stakeholders to embrace this Policy, which is a result of our joint efforts to date, and work together to develop our country and harness the power of ICTs in these efforts.

Moana CARCASSES KATOKAI KALOSIL
Prime Minister

National Cybersecurity Policy

1 Introduction

1.1 This National Cybersecurity Policy (the Policy) sets out the Goals, Policies and Objectives for the Republic of Vanuatu in maximizing safety and security in relation to the use of information and communication technology (ICT).

1.2 The Policy pays particular attention to the National ICT Policy, in particular priority 7.1 that defines principles related to Building Trust (Mitigating Risks and Threats related to ICT Development). It also reflect the aims of the Millennium Development Goals, draws upon the recommendations related to ICT arising from the Final Acts of the ITU Plenipotentiary Conference (Guadalajara, 2010), the ITU Global Cybersecurity Agenda and the results of work of the ICB4PAC project in relation to policy and legislation for Pacific Islands.

1.3 The Policy has been developed by a multi stakeholder group appointed by the Prime Minister in December 2012. The inaugural meeting was held in early February 2013 and since then have met 4 times. In addition to discussions among the members of working group, discussions were initiated with national, regional and international experts to ensure a broad participation including open stakeholder consultation.

1.4 The implementation of the Policy will be coordinated by the National Cybersecurity Steering Committee (NCSC) chaired by the DG responsible for ICT. The NCSC consists of public and private representatives (including non-profit organizations). Annex A sets out the Terms and Reference of the NCSC.

1.5 The DG of each Ministry will be responsible for developing action plans to achieve the objectives set out in this Policy.

1.6 The NCSC will prepare Annual Reports on the progress of implementing this Policy.

2 National Vision

Citizens of Vanuatu, tourists, businesses and government to enjoy the full benefits of a safe, secure and resilient cyberspace enabling them to get access to knowledge and share information while understanding and addressing the risks, to reduce the benefits to criminals.

2.1 With this vision we aim to protect the people, businesses and government and provide the necessary secure framework to achieve the aims developed and defined in the National ICT Policy.

2.2 To achieve this vision, we have identified five goals:

2.2.1 Develop the necessary organizational structures with a focus on utilizing existing structures in Vanuatu as well as the region;

2.2.2 Defining mandatory technical Cybersecurity minimum standards for operators of critical infrastructure and providing expertise as well as basic tools and services for citizens, businesses and government;

2.2.3 Strengthening the legal framework in Vanuatu to meet highest regional and international standards with regard to protection of fundamental rights as well as criminalization, investigation, electronic evidence and international cooperation;

2.2.4 Bringing the level of knowledge about Cybersecurity and ways to protect against cyber threats of the citizens and businesses of Vanuatu to highest levels; and

2.2.5 Responding to the global nature of Cybersecurity threats through strengthening Vanuatu's ability to participate in the international cooperation against such threats.

2.3 The government is aware that connecting to the submarine cable will have a major impact on the aims to connect more people in Vanuatu to the Internet. In addition the government is aware that with the increase in bandwidth new services will be available and that some of them will go along with security concerns. As a consequence the government gives priority to a timely implementation of the policy to ensure that Cybersecurity measures are implemented in parallel to the increase in services and connectivity.

Goals

GOAL 1 Develop the necessary organizational structures

Policy Statement: **Existing organizational structures within the country will be fostered, a National Computer Emergency Response Team (CERT) will be created and a strengthening of the cooperation with regional organizational structures like the PAC CERT will be evaluated.**

The objectives for Goal 1 are:

Objective 1 Create a National Cybersecurity Steering Committee (NCSC) chaired by the DG responsible for ICT. The NCSC will take the overall lead in the coordination of the implementation of the Cybersecurity policy and the process of carrying out the necessary tasks.

Objective 2 Identify all existing government and non-government institutions that are currently active in the field of Cybersecurity and fighting Cybercrime. Special attention should be paid to the identification of potential local points of contact in rural areas. Drafting of a report about the mandate, resources and experiences, and analysis of potential areas for synergy, overlapping and gaps.

Objective 3 Identify local contact points in rural areas that can facilitate the collection of input about recent developments as well as spreading information to the communities. Within this process public private partnership approaches shall be taken into consideration.

Objective 4 Establishment of a National Computer Emergency Response Team (CERT) that is capable of dealing with relevant Cybersecurity threats for citizens, tourists, businesses and government in Vanuatu. The CERT shall also provide computer forensic services within criminal investigations involving computer technology or electronic evidence. In addition the CERT shall be responsible to monitoring developments and ensuring that information about current trends and risks (such as Vanuatu specific phishing attacks or the detection of skimming devices in the country) are communicated through the different channels. Within the development of the national CERT a possible outsourcing of services to regional organizations such as PacCERT should be evaluated.

Objective 5 Create a child online protection working group (COPWG) to identify areas of child online protection (such as technical protection measures, curriculums for school and information material for parents and guardians) that need to be integrated in Vanuatu. The COPWG shall also evaluate different technical measures that services providers must introduce to protect children online and parameters that shall be included in a report submitted to guardians upon request (see GOAL 2, Objective 4). This shall include recommendations for measures how to prevent an abuse of the service. A report shall be submitted to the NCSC until December 2013.

Objective 6 Develop a strategy to encourage the reporting of Cybersecurity incidents. The increase of information shall feed into concrete warnings about recent trends, regular information about latest trends for press and general public and quarterly reports about the development of incidents for NCSC. Set up of a central website for reporting Cybersecurity incidents by businesses and citizens as well as providing information and tools.

Objective 7 Development of unit within law enforcement that serves as single point of contact for requests from government institutions as well as citizens and businesses. The creation of a contact point and the installation of the website shall increase the amount of information available.

Objective 8 To carry out a coordinated survey and assessment, to analyse how far citizens, businesses and government are affected by Cybersecurity incidents and Cybercrime

GOAL 2 Standardization and Services

Policy Statement: **Defining and controlling technical minimum standards for operators of national critical infrastructure to ensure basic security standards. Furthermore, provide services for citizens and businesses.**

The objectives for Goal 2 are:

Objective 1 Identify operators of national critical infrastructure and determine the use of ICT by those operators and the related risks.

Objective 2 Develop technical and organizational minimum standards for the operator of critical infrastructure and the related control/evaluation mechanisms to ensure that the risk of Cybersecurity related attacks are minimized.

Objective 3 The CERT shall carry out the same assessment and development of minimum standards as defined in objective 1 with regard to ICT operated and used by government institutions. This shall include

the identification of critical processes and the introduction of different security levels. Furthermore, the CERT shall be responsible for the implementation and control of the developed standards.

Objective 4 Through the CERT or other government services provide basic services to citizens and businesses that have needs in relation to Cybersecurity concerns. This shall include pointing out free of charge tools, providing information material in Bislama, as well as training courses. To carry out the activities public private partnerships (for example with local access provider and computer provider) should be evaluated.

Objective 5 Each commercial provider of Internet access in Vanuatu shall be obliged to provide — upon request of the user — a restricted Internet access that includes available technical measures aiming to block content that is not appropriate for children. Furthermore, the provider shall be obliged to provide — upon request of the user — a special reporting for parents or guardians that highlights the services used and other parameters defined by the Child Online Protection Working Group ("COPWG").

Objective 6 Each commercial provider of GSM mobile communication services in Vanuatu shall be obliged to provide — upon request — a SIM card with restricted access to services that may not be appropriate for children. The provider may not charge any additional fees for such service.

Objective 7 CERT will develop routines to detect recent trends in relation to Cybersecurity incidents such as, create an emergency level system, summarizing incidents in a reporting format and providing background information, developing a network to communicate such reports through the relevant communication channels (e.g. press releases, information submitted to cooperation partners in rural areas) and submitting this information. CERT shall ensure that the information submitted to the different stakeholders reflect their needs with regard to details (e.g. executive summary for the minister, detailed information for system administrators on technical aspects of an attack) and that information are not distributed to recipients that are not affected.

GOAL 3 Strengthening the legal framework

Policy Statement: **In order to protect openness and a safe environment Vanuatu shall have a reliable legal framework that reflects the uniqueness of the country as well as international best practices.**

The objectives for Goal 3 are:

Objective 1 Under supervision of NCSC a review of the existing legislation related to Cybersecurity and Cybercrime should be carried out. This shall include definitions, penal legislation, investigation instruments of law enforcement, admissibility of electronic evidence, liability of Internet Service Providers (ISPs), and specific provision to protect children online and international cooperation. The review shall include the identification of existing provisions that could be utilized in relation to Cybersecurity, a comparison with international best practices, a gap analysis, suggestions for amendments and the related drafting instructions. This activity shall be carried out in close cooperation with the State Law Office and built upon existing work carried out in the region (e.g. the assessment of legislation within the ICB4PAC project). A report including the drafting instructions shall be submitted until October 2013.

Objective 2 Based upon the report and the drafting instructions the State Law Office will prepare the draft legislation until December 2013.

GOAL 4 Capacity building

***Policy Statement:* Ensuring that all relevant stakeholders including citizens, students, businesses, judiciary, and law enforcement receive sustainable training.**

The objectives for Goal 4 are:

Objective 1 The Ministry of Education will in cooperation with NCSC and other authorities in Vanuatu develop a curriculum to ensure that all students at primary school and high school receive at least once a year an updated training on Cybersecurity that includes information about latest trends. The working group shall for the different age groups develop the related training materials, background information for teachers and sample presentations. In addition schools should receive a questionnaire to enable them to assess the use of ICT service by students as well child specific Cybersecurity risks. The anonymous assessment shall be carried out on an annual basis and the results shall be submitted to NCSC and included in their annual report.

Objective 2 Identify cooperation partner (such as chiefs and religious leaders) in rural areas that can support the capacity building initiatives by providing information about security within their daily work. Providing them with the necessary background information and training material.

Objective 3 Development of a sustainable training program for law

enforcement officers (police, customs), FIU, state law and the judiciary.

Objective 4 The State Law Office, judiciary and law enforcement agencies shall develop a national crime prevention strategy related to Cybercrime. The work shall be coordinated by NCSC to ensure that the measures discussed are in line with measures taken forward within other working groups (e.g. the creation of information material by the CERT).

GOAL 5 International Cooperation

Policy Statement: **To tackle the transnational dimension of Cybersecurity incidents on the one hand side and benefit from the support of different organizations for developing countries on the other hand side, Vanuatu will utilize means of international cooperation and support.**

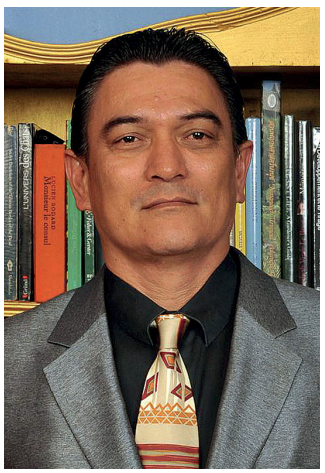
The objectives for Goal 5 are:

Objective 1 To ensure that Vanuatu's legal framework is fully in line with international best practices. The NCSC will analyse the capacities of Vanuatu to efficiently submit requests for mutual legal assistance as well as timely respond to requests submitted to authorities in the country. NCSC will develop recommendations for the establishment of a single point of contact. Further more the NCSC will analyse if the technology used for sending and receiving requests as well as the availability of the contact point are in line with international best practices.

Objective 2 NSCS will make recommendations with regard to a potential access to international or regional agreements, current processes of developing binding standards where Vanuatu should participate, as well as 24/7 networks (such as the G8 or Interpol Network). With regard to the evaluation of an access to existing instruments the relevance for Vanuatu, the reflection of legal standards and cultural specifies as well as the usefulness in cooperation with major countries such as the Australia, the US and China shall be taken into consideration.

Objective 3 NSCS shall provide a list of capacity building programs related to Cybersecurity that Vanuatu could benefit from. To avoid an overlapping NSCS shall develop a roadmap that lists the different capacity activities that the country require, identify potential programs and make suggestions which programs cover which activity.

Avant-propos



L'Honorable Moana CARCASSES KATOKAI KALOSIL, Premier ministre du République de Vanuatu

J'ai le plaisir de vous présenter la Politique de cyber-sécurité. Cette Politique témoigne de l'engagement du gouvernement à maximiser la sûreté et la sécurité des technologies de l'information et des communications afin de réaliser la vision nationale qui est de transformer Vanuatu en « une nation juste, instruite, saine et prospère », et ainsi valoriser et avantager tous les citoyens et résidents de Vanuatu.

L'engagement du gouvernement en cours se traduira tout d'abord par les buts fixés dans la présente politique afin de veiller à ce que les citoyens de Vanuatu, les touristes, les entreprises et le gouvernement jouissent des avantages entiers d'un cyberespace sûr, sécurisé et résistant qui leur permet d'avoir accès au savoir et de partager les informations tout en tenant compte des risques afin de réduire les avantages aux criminels. Cette politique favorise des actions et collaborations innovantes entre le secteur privé et le gouvernement pour une coordination et collaboration conjointe afin d'atteindre les buts de la politique.

Le projet d'installation de câbles à fibre optique sous-marins favorisera une connexion fiable à haute vitesse de Vanuatu au reste du monde. Cela signifie les usagers de l'Internet en général sont exposés aux risques expérimentés par les autres pays. Les institutions du secteur, en particulier le Groupe de travail multipartite de cyber-sécurité, le Bureau du Chef de service de l'information du gouvernement, le Régulateur des télécommunications et radiocommunications et les fournisseurs de services Internet (FSI) sont chargés d'une fonction stimulante de s'assurer que Vanuatu résiste bien à de telle cyber-attaque.

Au cours de notre travail, nous avons reçu des aides venant de plusieurs organisations internationales et régionales, ainsi que de nos partenaires au développement. Je tiens à remercier en particulier l'Union internationale des télécommunications (UIT) qui a constamment soutenu le développement institutionnel et le l'élaboration de politique dans le secteur de cyber-sécurité dans le pays, par l'intermédiaire du programme ICB4PAC conçu pour le Pacifique et dont Vanuatu est le bénéficiaire.

Beaucoup a été réalisé mais beaucoup reste encore à accomplir. Les TIC ont un grand potentiel de transformer l'éducation de nos enfants, d'élargir et d'améliorer les services du gouvernement. Elles nous aident à résister de plus en plus face aux catastrophes naturelles, nous permettent de préserver et promouvoir notre culture, nous offrent de nouvelles possibilités commerciales et améliorent, de manière générale, nos moyens de subsistance. Elles nous permettront de nous rapprocher des uns et des autres, et de renforcer notre connexion au reste du monde. Cependant, les vrais avantages dépendent des efforts que nous fournirons ensemble – le gouvernement, le secteur privé, le milieu universitaire, les utilisateurs, la société civile et en fin de compte, tous les citoyens et résidents. Ce n'est

qu'ensemble que nous pouvons transformer ce potentiel en une réalité que nous allons expérimenter tous les jours.

J'appelle donc toutes les parties prenantes à adopter cette politique qui est, à ce jour, le fruit des efforts que nous avons apporté en commun, puis à travailler ensemble pour développer notre pays et pour maîtriser la puissance des TIC par ces efforts.

Moana CARCASSES KATOKAI KALOSIL
Premier ministre

Politique nationale de cybersécurité

1 Introduction

1.1 La présente Politique nationale de cybersécurité expose les buts, objectifs et politiques de la République de Vanuatu, qui servent à optimiser la sûreté et la sécurité concernant l'utilisation des technologies de l'information et des communications (TIC).

1.2 La politique accorde une attention particulière à la Politique nationale des TIC, en particulier la priorité 7.1 qui définit les principes relatifs à l'établissement de la confiance (réduire les risques et menaces liées au développement des TIC). Elle reflète également les Objectifs du millénaire pour le développement, s'appuyant sur les recommandations relatives aux TIC soulignées dans les Actes finals de la Conférence de plénipotentiaires de l'UIT (Guadalajara, 2010), le Programme mondial cybersécurité de l'UIT et les résultats des travaux du projet ICB4PAC en lien avec la politique et loi pour les îles du Pacifique.

1.3 La politique a été élaborée par un groupe multipartite nommé par le Premier ministre en décembre 2012. La réunion inaugurale a eu lieu au début de février 2013 et depuis, il s'est encore réuni à quatre reprises. En plus des discussions entre les membres de ce groupe de travail, celles-ci ont également été entamées avec des experts nationaux, régionaux et internationaux afin d'obtenir une vaste participation, y compris des consultations ouverte avec les parties intéressées.

1.4 La mise en œuvre de la Politique sera coordonnée par le Comité directeur national de cybersécurité (CDNC), présidé par le DG délégué des TIC. Le CDNC est composé de représentants des secteurs public et privé (y compris les organisations à but non lucratif). L'annexe A expose les attributions du CDNC.

1.5 Les directeurs généraux de chaque ministère seront responsables de l'élaboration de plans d'action qui permettront d'atteindre les objectifs exposés dans la présente Politique.

1.6 Le CDNC établira des rapports annuels sur l'état d'avancement de la mise en œuvre de cette Politique.

2 Vision nationale

Les citoyens de Vanuatu, les touristes, les entreprises et le gouvernement doivent bénéficier de tous les avantages que peut offrir un cyber espace sûr, protégé et résilient qui leur permettra d'avoir accès au savoir et de partager de l'information, tout en tenant compte des risques afin de réduire les avantages aux criminels.

2.1 Par cette vision, nous visons à protéger les individus, les entreprises et le gouvernement, et à établir un cadre de sécurité nécessaire afin d'atteindre les objectifs élaborés et définis dans la Politique nationale des TIC.

2.2 Pour réaliser cette vision, cinq objectifs ont été identifiés :

2.2.1 Établir des structures organisationnelles nécessaires en se concentrant sur l'utilisation des structures existantes à Vanuatu ainsi que dans la région ;

2.2.2 Définir des normes minimales techniques obligatoires de cybersécurité pour les exploitants des infrastructures principales et fournir de l'expertise ainsi que des outils et services de base pour les citoyens, les entreprises et le gouvernement ;

2.2.3 Renforcer le cadre juridique à Vanuatu afin de répondre aux normes régionales et internationales les plus élevées en ce qui concerne la protection des droits fondamentaux ainsi que la criminalisation, l'enquête, la preuve électronique et la coopération internationale ;

2.2.4 Porter à un niveau plus élevé, aux citoyens et entreprises à Vanuatu, les connaissances sur la cybersécurité et les moyens de protection contre les cyber-menaces ; et

2.2.5 Répondre à la nature globale des menaces contre la cybersécurité en renforçant la capacité de Vanuatu à participer à la coopération internationale contre ces menaces.

2.3 Le gouvernement est conscient que la connexion par câble sous-marin aura un impact important sur les objectifs de connecter à Internet plus de personnes à Vanuatu. En outre, le gouvernement est conscient qu'avec la multiplication de la bande passante, de nouveaux services seront disponibles et dont certains accepteront les soucis de la sécurité. En conséquence, le gouvernement donne la priorité à une mise en œuvre opportune de la politique, afin de veiller à ce que les mesures de cybersécurité soient mises en œuvre parallèlement avec l'augmentation des services et de la connectivité.

Les Buts

1er BUT Établir des structures organisationnelles nécessaires

***Déclaration de* principes : Les structures organisationnelles existantes dans le pays seront promues, une Équipe nationale d'intervention en cas d'urgence informatique (CERT) sera créée et un renforcement de la coopération avec les structures organisationnelles régionales comme la PAC CERT sera évalué.**

Les objectifs du 1ier BUT sont les suivants :

Objectif 1 Créer un Comité directeur national de cybersécurité (CDNC), présidé par le DG délégué des TIC. Le CDNC assurera la supervision générale de la coordination de la mise en œuvre de la politique de cybersécurité et le processus de l'exécution des tâches nécessaires.

Objectif 2 Identifier toutes les institutions gouvernementales et non gouvernementales existantes qui sont actuellement actives dans le domaine de la cybersécurité et dans la lutte contre la cybercriminalité. Une attention particulière doit être accordée à l'identification de potentiels points de contact locaux dans les zones rurales. Rédiger un rapport sur le mandat, les ressources et les expériences ainsi que l'analyse détaillée des domaines potentiels en vue de la synergie, des recouvrements et des lacunes.

Objectif 3 Identifier des points de contact locaux dans les zones rurales qui peuvent faciliter la collecte de données sur les développements récents ainsi que la diffusion d'informations aux communautés. Dans ce processus, les approches de partenariat public-privé doivent être prises en considération.

Objectif 4 Créer une Équipe national d'intervention en cas d'urgence informatique (CERT) capable de traiter les menaces pertinentes de cybersécurité contre les citoyens, les touristes, les entreprises et le gouvernement de Vanuatu. La CERT doit également fournir des services d'informatique judiciaire dans le cadre d'enquêtes criminelles impliquant la technologie informatique ou la preuve électronique. En outre, la CERT sera chargé de surveiller les développements et de veiller à ce que l'information sur les tendances et les risques actuels (tels que les attaques spécifiques de filoutage ou la détection de dispositifs d'écrémage dans le pays) soit diffusée par

les différentes voix de communication. Dans le cadre de la création de la CERT nationale, une possible externalisation de services à des organisations régionales, telles que PacCERT, doit être évaluée.

Objectif 5 Créer un groupe de travail sur la protection en ligne des enfants (COP) afin d'identifier les domaines de la protection en ligne des enfants (tels que les mesures techniques de protection, les programmes scolaires et des matériels d'information pour les parents et tuteurs) qui doivent être incorporés au sein du pays. Il doit également évaluer les différentes mesures techniques que les fournisseurs de services doivent introduire pour protéger les enfants en ligne, et les paramètres qui doivent figurer dans un rapport soumis sur demande aux tuteurs (voir 2ème BUT, objectif 4). Ceci doit inclure des recommandations pour des mesures visant à prévenir une utilisation abusive du service. Un rapport doit être soumis à la CDNC d'ici décembre 2013.

Objectif 6 Élaborer une stratégie pour encourager le signalement des incidents liés à la cybersécurité. L'augmentation de l'information doit alimenter des avertissements concrets sur les tendances récentes, des informations régulières sur les tendances récentes pour la presse et le grand public, ainsi que des rapports trimestriels au CDNC sur le développement des incidents. Créer un site Web central qui sera utilisé par les entreprises et citoyens pour signaler les incidents qui ont trait à la cybersécurité, ainsi que pour fournir des informations et outils.

Objectif 7 Créer une section, dans le cadre de l'application de la loi, qui servira de point de contact unique pour les demandes des institutions gouvernementales ainsi que des citoyens et entreprises. La création d'un point de contact et du site augmentera la quantité des informations disponibles.

Objectif 8 Mener à bien une étude et évaluation coordonnée, afin d'analyser à quel point les citoyens, les entreprises et le pouvoir public sont touchés par des incidents liés à la cybersécurité et cybercriminalité.

2ème BUT Uniformisation et services

***Déclaration de* principes : Définir et contrôler les normes techniques minimales pour les exploitants des infrastructures nationales essentielles afin d'assurer des normes de sécurité de base. En outre, fournir des services aux citoyens et aux entreprises.**

Les objectifs du 2ième BUT sont les suivants :

Objectif 1 Identifier les exploitants des infrastructures essentielles nationales et déterminer l'utilisation des TIC par ces exploitants et les risques

afférents.

Objectif 2 Établir des normes minimales techniques et organisationnelles pour l'exploitant de l'infrastructure essentielle et des mécanismes connexes de contrôle et d'évaluation afin de s'assurer que les risques d'attaque liées à la cybersécurité soient minimisés.

Objectif 3 La CERT doit effectuer la même évaluation et établir les mêmes normes minimales, comme dans le 1er objectif, en ce qui concerne les TIC exploitées et utilisées par les institutions gouvernementales. Ceci doit inclure l'identification des processus critiques et l'introduction de différents niveaux de sécurité. En outre, la CERT est responsable de la mise en œuvre et du contrôle des normes établies.

Objectif 4 Par l'intermédiaire de la CERT ou des autres services gouvernementaux, fournir des services de base aux citoyens et entreprises qui se soucient de la cybersécurité. Ceci doit inclure l'offre des outils gratuits, des instruments d'information en bichlamar, ainsi que des formations. Afin d'effectuer ces activités, les partenariats publics-privés (par exemple entre un fournisseur à accès local et un commerçant d'ordinateur) doivent être évalués.

Objectif 5 Chaque fournisseur d'accès Internet à Vanuatu est tenu de fournir, sur demande de l'utilisateur, un accès Internet restreint qui comprend des mesures techniques disponibles visant à bloquer des contenus non appropriés aux enfants. En outre, le fournisseur est tenu de fournir, sur demande de l'utilisateur, une déclaration spéciale pour les parents ou tuteurs, mettant en valeur les services utilisés et d'autres paramètres définis par le groupe de travail COP. Le prix de l'accès à Internet ne peut pas être plus élevé que les 10% de l'accès régulier.

Objectif 6 Chaque fournisseur de service de communication par téléphone GSM à Vanuatu est tenu de fournir, sur demande, une carte SIM avec un accès qui limite les services non appropriés aux enfants. Le fournisseur peut ne pas facturer de frais supplémentaires pour ce service.

Objectif 7 La CERT déterminera des routines de détection de tendances récentes en ce qui concerne les incidents liés à la cybersécurité, tel que la création d'un système de niveau d'urgence, le résumé des incidents sous format de compte rendu et l'apport des informations de base, l'établissement d'un réseau servant à communiquer ces rapports par le biais des voix de communication pertinentes (par exemple, les communiqués de presse pour les informations diffusées aux partenaires de la coopération dans les zones rurales) et la soumission de ces informations. La CERT doit s'assurer que les renseignements fournis aux différents acteurs répondent à leurs

besoins en ce qui concerne les détails (par exemple, le résumé du ministre, des informations détaillées pour les administrateurs du système sur les aspects techniques d'une attaque) et que les informations ne soient pas distribuées aux destinataires non touchés.

3ème BUT Consolidation du cadre juridique

***Déclaration de* principes : Afin de protéger l'ouverture et un environnement sûr, Vanuatu doit disposer d'un cadre juridique fiable qui reflète le caractère unique du pays ainsi que les meilleures pratiques internationales.**

Les objectifs du 3ième BUT sont les suivants :

Objectif 1 Sous la supervision du CDNC, un examen de la loi existante relative à la cybersécurité et la cybercriminalité doit être effectué. Ceci doit inclure des définitions, la législation pénale, les instruments d'enquête des exécuteurs de la loi, la recevabilité de la preuve électronique, la responsabilité des fournisseurs d'accès Internet (FAI), ainsi qu'une disposition spécifique sur la protection des enfants en ligne et la coopération internationale. L'examen doit comprendre l'identification des dispositions existantes qui pourraient être utilisées dans le cadre de la cybersécurité, une comparaison avec les meilleures pratiques internationales, une analyse des écarts, des suggestions de modifications et les consignes connexes de rédaction. Cette activité sera menée en étroite coopération avec le Cabinet juridique de l'État et s'appuiera sur les travaux existants réalisés dans la région (par exemple, l'évaluation de la législation dans le cadre du projet ICB4PAC). Un rapport contenant les consignes de rédaction doit être soumis d'ici octobre 2013.

Objectif 2 D'ici décembre 2013, le Cabinet juridique de l'État se basera sur le rapport et les consignes de rédaction afin de préparer le projet de loi.

4ème BUT Renforcement des capacités

***Déclaration de* principes : Veiller à ce que les parties prenantes pertinentes, y compris les citoyens, les étudiants, les entreprises, le secteur judiciaire et de l'exécution de la loi reçoivent des formations continues.**

Les objectifs du 4ième but sont les suivants :

Objectif 1 Le ministère de l'Éducation, en collaboration avec le CDNC et d'autres autorités à Vanuatu, doit élaborer un programme qui permettra aux élèves des écoles primaires et secondaires de recevoir au moins une fois par an, une formation à jour sur la cybersécurité qui contient des informations sur les dernières tendances.

Le groupe de travail doit élaborer le matériel nécessaire à la formation de différents groupes d'âge, préparer des informations générales pour les enseignants et créer un modèle de présentation. En outre, les écoles doivent recevoir un questionnaire qui les aidera à évaluer l'utilisation des services TIC par les élèves, ainsi que les risques de cybersécurité spécifiques à l'enfant. L'évaluation anonyme doit être effectuée sur une base annuelle et les résultats doivent être soumis au CDNC et inclus dans leur rapport annuel.

Objectif 2 Identifier les partenaires de coopération (tels que les chefs coutumiers et les autorités religieuses) dans les zones rurales qui peuvent soutenir les initiatives de renforcement des capacités, en fournissant des informations sur la sécurité dans le cadre de leur travail quotidien. Et leur apportant des informations de base nécessaires ainsi que le matériel de formation.

Objectif 3 Élaborer un programme de formation continue pour les agents d'exécution de la loi (police, douane), l'UEF, le Cabinet juridique de l'État et le système judiciaire.

Objectif 4 Le Cabinet juridique de l'État, le secteur judiciaire et d'exécution de la loi doivent élaborer une stratégie nationale de prévention du crime liée à la cybercriminalité. Le travail sera coordonné par le CDNC pour s'assurer que les mesures débattues soient en accord avec les mesures appliquées au sein d'autres groupes de travail (par exemple, la production du matériel d'information par la CERT).

5ème BUT Coopération internationale

***Déclaration de* principes : Afin de mesurer aussi bien l'étendue multinationale des incidents de cybersécurité que les avantages de l'appui apporté aux pays en développement par différentes organisations, Vanuatu utilisera des moyens de coopération et d'aide internationale.**

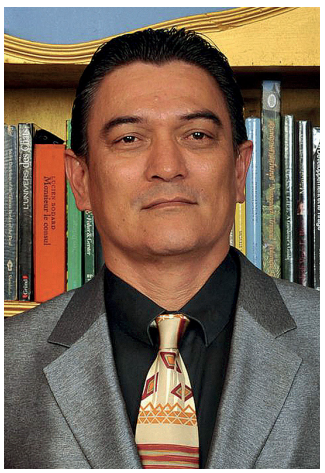
Les objectifs du 5ième but sont les suivants :

Objectif 1 S'assurer que le cadre juridique de Vanuatu est bien en accord avec les meilleures pratiques internationales. Le CDNC analysera les capacités de Vanuatu de soumettre, avec efficacité, des demandes d'entraide juridique, ainsi que des réponses opportunes aux demandes soumises aux autorités du pays. Le CDNC apportera des recommandations pour l'établissement d'un point de contact unique. De plus, le CDNC va analyser si la technologie utilisée pour l'envoi et la réception des demandes, ainsi que la disponibilité du point de contact, sont en accord avec les meilleures pratiques internationales.

Objectif 2 Le CDNC apportera des recommandations concernant un accès potentiel à des accords internationaux ou régionaux, des processus actuels d'établissement de normes obligatoires auquel Vanuatu doit participer, ainsi que des réseaux 24/7 (tels que le réseau du G8 ou le réseau Interpol). En ce qui concerne l'évaluation d'un accès aux instruments existants, la pertinence de Vanuatu, le reflet de normes juridiques et des spécificités culturelles, ainsi que l'utilité de la coopération avec les grands pays tels que l'Australie, les États-Unis et la Chine doivent être pris en considération.

Objectif 3 Le CDNC doit fournir une liste de programmes de renforcement des capacités liées à la cybersécurité desquels Vanuatu pourrait bénéficier. Pour éviter de chevauchement, le CDNC doit élaborer une feuille de route qui répertorie les différentes activités de renforcement des capacités que le pays a besoin, identifier d'éventuels programmes et apporter des suggestions concernant quel programme couvre quelle activité.

Festok



Hon. Moana Carcasses Katokai Kalosil, Praem Minista blong Vanuatu

Mi glad blong prisentem long yufala Saebasekiuriti Polisi ia. Polisi ia hemi talemaot strong komitmen blong Gavman blong maximaesem kontribiusen, efisiensi mo efektivnes blong ol infomeisen mo komiunikeisen teknoloji blong ajivim Nasonal Visen blong gat wan " Wan Vanuatu we i fea, i kasem gud edukeisen, i helti mo i rij", mo givim paoa mo benefit long evri sitisen mo residen blong Vanuatu.

Komitmen blong Gavman ia bae i kamaot fastaem tru long ol gol we bae oli setemaot insaed long polisi ia blong mekemsua se ol sitisen blong Vanuatu, ol turis, bisnis mo gavman oli enjoem ful benefit blong wan sef, sekua, mo resilien saeba speis we i mekem olgeta oli save gat akses long save, shearem infomeisen mo long semtaem andastanem mo adresem olgeta risk, blong ridiusum ol benefit long ol kriminol. Polisi ia i mekem se i gat strong kolaboreisen mo aksem bitwin praevet sekta mo gavman blong oli wok tugeta blong ajivim olgeta gol blong polisi ia.

Projek blong Interchange Sabmarin Kebol bae i givim wan hae-spid rilaeabol link blong Vanuatu long Wol. Hemia i minim se olgeta we oli stap yusum intanet bae oli expos long ol risk we ol narafala kaontri oli stap fesem. Jalensing wok blong mekemsua se Vanuatu i save fesem mo kamaot long olgeta saeba atak ia i stap long hand blong olgeta sekta institusen olsem malti-steholda Cybersecurity Working Group, Ofis blong Jif Infomeisen Ofisa blong Gavman, Telekomiunikeisen mo Radiokomiunikeisen Reguleita, olgeta Intanet Sevis Provaeda (ISP).

Long wok blong yumi yu enjoem sapot blong olgeta fren blong yumi blong plante intanasonal mo rijinol oganaeseisen, mo ol divelopmen patna blong yumi. Mi wantem talem wan spesel tangkio long International Telecommunications Union (ITU), we i stap sapotem oltaem institusenal mo polisi divelopmen long eria blong Saebasekiuriti long Vanuatu, tru long ICB4PAC program blong blong ol Pasifik Aelan we Vanuatu i stap benefit long hem.

Yumi ajivim plante samting finis. Be, i gat plante samting yet blong mekem. Ol IKT oli gat strong potensol blong jenisim edukeisen blong ol pikinini blong yumi, expandem mo impruvum ol sevis blong gavman, mekem yumi kam moa resilien long taem blong ol natural disasta, prisevem mo promotem kalja blong yumi mo tu provaedem ol niu bisnis opotuniti mo long jenerol leftemap laef blong yumi. Bambae oli bringim yumi i kam kolosap long yumi moa mo strentenem koneksen blong yumi long Wol. Be, actual benefit bae i dipen sipos yumi evriwan i wok tugeta – Gavman, ol bisnis, academia, ol yusa, sivil sosaeti mo long en, evri sitisen mo residen. Sipos yumi wok tugeta nomo bambae yumi save mekem potensol ia i kam rialiti we bae yumi save filim evri dei.

Mi stap askem evri stekholda blong oli oli tekem Polisi ia, we hemi risalt

blong olgeta joen efot blong yumi kasem naoia, mo blong wok tugeta blong divelopem kaontri blong yumi mo blong givim paoa long ol IKT.

Moana CARCASSES KATOKAI KALOSIL
Praem Minista

Nasonal Cybersekuriti Polisi

1 Introdaksen

1.1 Nasonal Cybersekuriti Polisi ia (Polisi) hemi aotlaenem ol Gol, ol Polisi mo ol Objektiv blong Ripablik blong Vanuatu blong inkrisim seifti mo sekuriti konsenem yus blong infomeisen mo komunikeisen teknoloji (ICT).

1.2 Polisi hemi givim patikula atensen long Nasonal ICT Polisi, spesieli praeoriti 7.1 we hemi identifaem ol prinsipol wetem Bilding Trast (Mitigating Risk mo Tret long ICT Divelopmen). Hemi riflektem tu eim blong Milenium Divelopmen Gol, we i kamaot long ol rikomendeisen we i stap long ol Faenol Akt blong ITU Plenipotensieri konferens (Guadalajara, 2010), ITU Globol Cybersekuriti Ajenda mo ol risal blong wok blong ICB4PAC projekt konsenem polisi mo legislesen blong Pasifik Aelan.

1.3 Wan malti stekholda grup we Praem Minista hemi bin apoentem long Disemba 2012 hemi bin divelopem polisi ia. Oli holem fes miting long eli manis blong februari 2013 mo sins long taem ia oli bin mit 4 taem. Antap long ol diskasen bitwin ol memba blong ol woking grup, ol nasonal, rijenol mo intenasonal ekspet oli inisietem ol diskasen inkludim open stekholda konsaltesen.

1.4 Nasonal Cybersekuriti Stering Komiti (NCSC) we DG we hemi risponsibol long ICT hemi hedem, hem nao hemi kodinetem implimentesen blong Polisi. NCSC hemi tekem tugeta pablik mo praevet ripresentetiv (inkludim ol non-profit oganaesesen). Anex A hemi putumaot ol Tem mo Riferens blong NCSC.

1.5 DG blong wanwan Ministri bae hemi risponsibol blong divelopem ol aksen plan blong ajivim ol objektiv we i stap long Polisi ia.

1.6 NCSC bae hemi priperem ol Anuol Ripot long progres blong implimentem Polisi ia.

2 Nasonal Visen

Ol sitisen blong Vanuatu, ol turis, ol bisnis mo gavman blong enjoyem ful benefit blong wan seif, sekiu mo fleksibol cyber spes blong mekem se oli gat akses long save mo sherem infomeisen wael andastaning mo adresem ol risk, blong rediusim ol benefit blong ol kriminol.

2.1 Wetem visen ia yumi eim blong protektem ol pipol, ol bisnis mo gavman mo provaedem neseseri sekiu framwok blong ajivim ol eim we oli divelopem mo difaenem long Nasonal ICT Polisi.

2.2 Blong ajivim visen ia, yumi identifaem 5 gol:

2.2.1 Divelopem neseseri oganaesesenol strakja wetem wan fokas blong yusum ol eksisting strakja long Vanuatu mo long rijen;

2.2.2 Difaenem mandatori teknikol Cybersekuriti minimum standed blong ol opereta blong kritikol infrastrakja mo provaedem ekspetis mo ol besik tul mo sives blong ol sitisen, ol bisnis mo gavman;

2.2.3 Reinfosem ligol framwok long Vanuatu blong mitim hae rijenol mo intenasonal standed blong protektem ol fandamentol raet mo tu ol kriminol aktiviti, investigeisen, elektronik evidens mo intenasonal koperesen;

2.2.4 Tekem level blong save abaot Cybersekuriti mo ol wei blong protektem akensem cyber tret blong ol sitisen mo bisnis blong Vanuatu long hae level; mo

2.2.5 Riplae long globol neija blong ol Cybersekuriti tret tru long wei blong mekem i kam strong moa abiliti blong Vanuatu blong tekpat long intenasonal koperesen akensem ol tret olsem.

2.3 Gavman hemi awea se blong konekt long sabmarine kebol bae hemi gat wan bigfala impakt long ol eim blong konektem moa pipol long Vanuatu long Intenet. Antap long hem, gavman hemi awea se wetem inkris long bandwidth wetem niu sevis bae hemi availebol mo sam long olgeta bae oli go wetem ol sekuriti konsen. Olsem risal, gavman hemi givim praeoriti long wan taemli implimentesen blong polisi blong mekem sua se oli implimentem ol step blong Cybersekuri semak olsem inkris long sevis mo konektiviti.

Ol Gol

GOL 1 Divelopem ol neseseri oganaesesenol strakja

Polisi Stetmen: **Bae oli promotem eksisting oganaesesenol strakja insaed long kaontri, bae oli krietem wan Nasonal Kompiuta Emejensi Rispons Tim (CERT) mo bae oli mekem i kam strong moa koperesen wetem ol rijenol oganaesesenol strakja olsem we bae oli asesem PAC CERT.**

Ol objektiv blong Gol 1 hemi:

Objektiv 1 Krietem wan Nasonal Cybersekuriti Stering Komiti (NCSC) we DG we hemi risponsibol long ICT hemi hedem. NCSC bae hemi tekem ovarol lid long kodinesen blong implimentesen blong Cybersekuriti polisi mo proses blong karemaot ol neseseri wok.

Objektiv 2 Identifaem evri eksisting gavman mo non-gavman institusen we oli aktiv naoia long fil blong Cybersekuriti mo faet akensem Cyberkraem. Oli shud givim spesol atensen long identifikeisen blong ol potensol lokol poen blong kontakt long ol rurol eria. Drafting blong wan ripot abaot mandet, risos mo eksperiens mo analisis blong ol potensol eria blong synerji, ovalaping mo gap.

Objektiv 3 Identifaem ol lokol kontakt poen long ol rurol eria we oli save fasilitetem koleksen blong input abaot risent divelopmen mo tu blong pasem infomeisen long ol komuniti. Insaed long proses ia oli save konsiderem pablik praevet patnasip aproj.

Objektiv 4 Establismen blong wan Nasonal Kompiuta Emejensi Rispons Tim (CERT) we hemi save dil wetem ol stret Cybersekuriti tret blong ol sitisen, turis, bisnis mo gavman long Vanuatu. CERT hemi save provaedem tu kompiuta forensic sevis insaed long ol kriminol investigesen we hemi involvem kompiuta teknoloji o elektronik evidens. Antap long hem CERT hemi shud risponsibol blong moniterem ol divelopmen mo meksua se infomeisen abaot karent trend mo risk (olsem Vanuatu spesifik phishing atak o detensen blong skiming divaes long kaontri) oli komuniket tru long ol difren janel. Insaed long divelopmen blong nasonal CERT, wan posibol sabkontrakt blong ol sevis blong ol rijenol oganaesesen olsem se oli shud evaluetem PacCERT.

Objektiv 5 Krietem wan pikinini onlaen proteksen woking grup (COPWG) blong identifaem ol eria blong pikinini onlaen proteksen (olsem teknikol proteksen step, kurikulum blong skul mo infomeisen materiol blong ol parens mo guadien) we oli nid blong integretem olgeta long Vanuatu. COPWG hemi shud evaluetem tu ol diferen teknikol step we ol sevis provaeda oli mas introdiusim blong protektem ol pikinini onlaen mo ol paramita we oli shud inkludim long wan ripot we oli sabmitim long ol guadien folem rikwest (luk long GOL 2, Objektiv 4). Hemia hemi shud inkludim ol rikomendesen blong ol step olsem wanem blong preventem wan abius blong sevis. Oli shud sabmitim wan ripot long NCSC kasem Disemba 2013.

Objektiv 6 Divelopem wan strateji blong encouragem ripoting blong ol Cybersekuriti insiden. Inkris blong infomeisen hemi shud givim konkret woning abaot ol risent trend, regula infomeisen abaot ol niu trend blong pres mo jenerol pablik mo ol kwateli ripot abaot divelopmen blong ol insiden blong NCSC. Ol bisnis mo sitisen oli setemap wan sentrol websaet blong ripotem Cybersekuriti insiden mo tu provaedem infomeisen mo ol tul.

Objektiv 7 Divelopmen blong yunit insaed long loa enfosmen we hemi sev olsem singel poen blong kontakt blong ol rikwest blong ol gavman institusen mo tu ol sitisen mo ol bisnis. Kriesen blong wan kontakt poen mo instolesen blong websaet hemi shud inkrisim amaon blong infomeisen we hemi availebol.

Objektiv 8 Blong karemaot wan sevei mo asesmen we oli kodinetem, blong analaesem olsem wanem ol Cybersekuriti insiden mo Cyberkraem oli afektem ol sitisen, bisnis mo gavman.

GOL 2 Standardiseisen mo Sevis

***Polisi Stetmen:* Difaenem mo kontrolem teknikol minimum standed blong ol opereta blong nasonal kritikol infrastrakja blong mekem sua se i gat ol besik sekuriti standed. Moa tu, provaedem ol sevis blong ol sitisen mo bisnis.**

Objektiv blong Gol 2 hemi:

Objektiv 1 Identifaem ol opereita blong nasonal kritikol infrastrakja mo detemaenem yus blong ICT we ol opereta ia oli mekem mo ol risk we i folem.

Objektiv 2 Divelopem teknikol mo oganaesesenol minimum standed blong opereta blong kritikol infrastrakja mo ol semak kontrol/evaluesen mekanisim blong mekem sua se oli limitim risk blong Cybersekuriti atak.

Objektiv 3 CERT hemia shud karemaot semak asesmen mo divelopmen blong

minimum standed olsem we i stap long objektiv 1 we ICT hemi operetem mo ol gavman institusen oli yusum. Hemia hemi shud inkludim identifikeisen blong ol kritikol proses mo introdaksen blong ol diferen sekuriti level. Moa tu, CERT hemi shud risponsibol long implimentesen mo kontrol blong ol divelop standed.

Objektiv 4 Tru long CERT o ol nara gavman sevis i givim ol besik sevis long ol sitisen mo ol bisnis we oli gat nid folem ol Cybersekuriti konsen. Hemia hemi shud indiketem se ol tul i fri, hemi provaedem infomeisen materiol long Bislama mo tu ol trening kos. Blong karemaot ol aktiviti pablik praevet patnasip oli shud evaluetem (olsem eksampol wetem lokol akses provaeda mo kompiuta provaeda).

Objektiv 5 Wanwan komesol provaeda blong Intenet akses long Vanuatu hemi shud gat obligesen blong provaedem — folem rikwest blong yusa — wan restrikted Intenet akses we hemi inkludim availebol teknikol step we hemi eim blong blokem kontent we hemi no apropriet long ol pikinini. Moa tu, provaeda hemi shud gat obligesen blong provaedem — folem rikwest blong yusa — wan spesol ripoting blong ol parens o gadien we hemi haelaetem ol sevis we oli yusum mo ol nara paramita we COPWG hemi difaenem. Praes blong Intenet akses hemi no save bitim 10% blong regula Intenet akses.

Objektiv 6 Wanwan komesol provaeda blong GSM mobael komunikeisen sevis long Vanuatu hemi shud gat obligesen blong provaedem — folem rikwest — wan SIM kad wetem restrikted akses long ol sevis we hemi no apropriet long ol pikinini. Provaeda hemi no save jajem eni adisonol fi blong kaen sevis olsem.

Objektiv 7 CERT bae hemi divelopem ol routine blong ditektem ol risent trend konsenem ol Cybersekuriti insiden olsem, krietem wan emejensi level sistem, samaraesem ol insiden long wan ripoting fomat mo provaedem bakraon infomeisen, divelopem wan netwok blong komuniket olsem ol ripot tru long ol stret komunikeisen janel(e.g. pres rilis, infomeisen we oli sabmitim long ol koperesen patna long ol rurol eria) mo sabmitim infomeisen ia. CERT hemi shud mekem sua se infomeisen we oli sabmitim long ol diferen stekholda hemi riflektem nid blong olgeta folem ol ditel (e.g. eksekutif samari blong minista, ditel infomeisen blong ol sistem administreta long ol teknikol aspekt blong wan atak) mo infomeisen ia oli no distributim long ol resipien we oli no afekted.

GOL 3 Strengthenem ligol framwok

Polisi Stetmen: **Blong protektem openes mo wan seif envaeraenem, Vanuatu hemi shud gat wan rilaebol ligol framwok we hemi soem se Vanuatu hemi yunik mo tu top intenasonal praktis.**

Objektiv blong Gol 3 hemi:

Objektiv 1 Anda long supevisen blong NCSC, wan riviu blong eksisting legislesen konsenen Cybersekuriti mo Cyberkraem oli shud karemaot. Hemia hemi shud inkludim ol definisen, penal legislesen, investigeisen instrumen blong loa enfosmen, admisibiliti blong elektronik evidens, laebiliti blong Intenet Sevis Provaeda (ISPs), mo spesifik provisen blong protektem ol pikinini onlaen mo intenasonal koperesen. Riviu hemi shud inkludim identifikeisen blong ol eksisting provisen we oli save yusum long Cybersekuriti, wan komparisen wetem top intenasonal praktis, wan gap analisis, ol proposol blong ol amenmen mo ol drafting instraksen. Oli shud karemaot aktiviti ia wetem sapot blong Steit Loa Ofis mo divelopem folem eksisting wok we oli karemaot long rijen (e.g. asesmen blong legislesen insaed long ICB4PAC projekt). Wan ripot inkludim ol drafting instraksen oli shud sabmitim kasem Oktoba 2013.

Objektiv 2 Bes long ripot mo ol drafting instraksen, Steit Loa Ofis bae hemi priperem draft legislesen kasem Disemba 2013.

GOL 4 Kapasiti bilding

***Polisi Stetmen:* Blong mekem sua se evri stekholda inkludim ol sitisen , ol bisnis, judisieri, mo loa enfosmen oli risivim sastenebol trening.**

Ol objektiv blong Gol 4 hemi:

Objektiv 1 Ministri blong Edukeisen wetem sapot blong NCSC mo ol nara otoriti long Vanuatu oli divelopem wan kurikulum blong mekem sua se evri studen long praemeri skul mo hae skul oli risivim wan taem long wan yia wan apdet trening long Cybersekuriti we hemi inkludim infomeisen abaot ol niu trend. Woking grup i shud divelopem blong ol diferen ej grup, ol semak trening materiol, bakraon infomeisen blong ol tija, eksampol blong ol prisentesen. Antap long hem, ol skul oli shud risivim sam kwesten blong mekem se ol studen oli gat akses long yus blong sevis blong ICT mo tu ol pikinini spesifik Cybersekuriti risk. Oli shud karemaot wan asesmen we oli no nemem long wan anuol besis mo oli shud sabmitim ol risal long NCSC mo inkludim long anuol ripot blong olgeta.

Objektiv 2 Identifaem koperesen patna (olsem ol jif mo ol jioj lida) long ol rurol eria we oli save sapotem kapasiti bilding inisietiv blong provaedem infomeisen abaot sekuriti insaed long evri dei wok blong olgeta. Provaedem long olgeta neseseri bakraon infomeisen mo trening materiol.

Objektiv 3 Divelopmen blong wan sastenbol trening program blong ol loa enfosmen ofisa (polis, kastoms), FIU, Steit Loa Ofis mo Judisieri.

Objektiv 4 Steit Loa Ofis, judisieri mo ol loa enfosmen ejensi oli shud divelopem wan nasonal kraem privensen strateji konsenem Cybersekuriti. NCSC hemi shud kodinetem wok blong mekem sua se ol step we oli tokbaot bae hemi inlaen wetem ol step we oli tekem long ol nara woking grup (e.g. CERT hemi krietem infomeisen materiol).

GOL 5 Intenasonal Koperesen

***Polisi Stetmen:* Blong takelem transnasonal dimensen blong Cybersekuriti indisen long wan saed mo benefit long sapot blong ol diferen oganaesesen blong ol diveloping kaontri long nara saed, Vanuatu bae hemi yusum ol mins blong intenasonal koperesen mo sapot.**

Objektiv blong Gol 5 hemi:

Objektiv 1 Blong mekem sua se ligol framwok blong Vanuatu hemi fuli inlaen wetem ol top intenasonal praktis. NCSC bae hemi analaesem ol kapasiti blong Vanuatu blong sabmitim gud ol rikwest blong wan mutuol ligol asistens mo tu stret rispon long ol rikwest we oli sabmitim long ol otoriti long kaontri. NCSC bae hemi divelopem ol rikomendeisen long establismen blong wan singel poen blong kontakt. Moa tu NCSC bae hemi analaesem sapos teknoloji we oli yusum blong sendem mo risivim ol rikwest mo tu availabiliti blong kontakt poen oli inlaen wetem ol top intenasonal praktis.

Objektiv 2 NSCS bae hemi mekem ol rikomendeisen folem wan potensol akses long ol intenasonal o rejinol agrimen, ol karent proses blong diveloping binding standed we Vanuatu i shud tekpat, mo tu 24/7 netwok (olsem G8 o Interpol Netwok). Folem evaluesen blong wan akses long eksisting instrumen long relevens blong Vanuatu, refleksen blong ligol standed mo ol kaljurol spesifae mo tu gudfala koperesen wetem ol bigfala kaontri olsem Ostrelia, US mo Jaena we oli shud konsiderem gud.

Objektiv 3 NSCS hemi shud provaedem wan list blong kapasiti bilding program konsenem Cybersekuriti we Vanuatu hemi save benefit long hem. Blong avoidem wan ovalaping, NCSC hemi shud divelopem wan rodmap we hemi listim ol diferen kapasiti aktiviti we kaontri hemi nidim, identifaem ol potensol program mo mekem ol proposol we program hemi kavremap aktiviti.

Graphic design by **Blue Planet Media + Communications** | info@blueplanet.vu