PAMBANSANG PUNONGHIMPILAN TANOD BAYBAYIN NG PILIPINAS
(National Headquarters Philippine Coast Guard)
139 25th Street, Port Area,
1018 Manila

NHQ-PCG/CG-11 **07 October 2019**

CIRCULAR
NUMBER 11-19

PHILIPPINE COAST GUARD CYBERSECURITY POLICY

I. REFERENCES:

a. PCG Regulations G200 – 001, (Security of classified matters) Dated 23 Sept 2002.

b. GHQ Letter directive Nr 287 dated 30 August 2013, Subj; Adopting cyberspace as one of the domains of AFP Operations.

c. CEIS Directive 2012-001, Subj: PN Standard LAN and network security.

d. National Cyber Security Plan 2022.

e. ISO 27002, Code of Practice for information Security Controls.

f. Certificated Information Systems Security Professional V1.1

g. NHQ-PCG/CG11 Standard Operating Procedures (SOP) Nr.: 05-19 (Utilization of PCG Provided Email Services).

h. NHQ-PCG/CG11 Standard Operating Procedures (SOP) Nr.: 09-19 (Utilization of issued PCG Mobile / Cellular Phones

i. Executive Order No. 189, s. 2015 – Creating The National Cybersecurity Inter-agency Committee

j. United States Coast Guard Cyber Strategy

II. PURPOSE:

The purpose of this policy is to govern set of principles, provide rules and higher guidance by which PCG organic personnel, civilian employees, third party stakeholder who are given access to the PCG Information infrastructures (infostructure) assets must abide, inform their obligatory requirements, limitations, privileges and responsibilities.

This publication shall serve as covenant and basis for the issuance of specific procedures, and guidelines to efficiently and effectively implement cyber security best practices and norms. This will provide directions and strategic priorities; framework enablers; promote confidence for both interagency and regional collaborations; and develop and leverage a diverse set of cyber capabilities and authorities.

Finally, this will provide a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions in attaining PCG mandated functions

III. SCOPE:

This policy provides guidance to administrators, maintainers, operation, and third-party stakeholder of the PCG C4IS infostructure for effective administration, operations, maintenance, and security of C4IS system.

IV. DEFINITION OF TERMS:

a. **Administrator** - Refers to the person responsible for managing the PCG network. The responsibilities of the administrator typically include installing and upgrading software; and backup and recovery tasks.

b. **Baseline Configuration –** is a fixed reference in the development cycle or an agreed-upon specification of a system at a point in time. It serves as a documented basis for defining incremental change and encompasses many different aspects of the system. It is the center of an effective configuration management program whose purpose is to give a definite basis for change control in a project controlling various configuration items like work, system performance and other measurable configuration, basically, it is a defined specification that is considered as the baseline for all changes that follow.

c. **Bring Your Own Device (BYOD)** – portable computing device – such as smartphones, laptops ad table – brought by personnel to the workplace for use and connectivity to the PCG network.

d. **Closed Network (Red network) –** Also known as the PCG RED network, this refers to the PCG internet makes use of the Virtual Private Network (VPN). It is a closed and secured network, and not accessible via internet. This shall be primarily used for internal communications and mission-critical information system of the organization.

e. **Confidential/Restricted (CONRES)** – Term used for the categorization of electronic document, computer system, service, storage, and mobile devices contained or stored with confidential or restricted information.

f. **Controlled Open Public Network (Network) –** also known as the PCG Network (Gray Network), the network that is open to the internet. It is an open and public yet a secured network. This shall be used for internet browsing and internet-facing applications such as the PCG website and the PCG collaboration suite (PCGCS), or PCG Emails System.

g. **Cyberspace** – used to described the virtual world of computers

h. **Cybersecurity** – refers to the collection of tools, policies, risk management, approaches, actions, trainings, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.

i. **C4IS Infrastructure -** refers to command, control, communications, computer, intelligence, surveillance, target acquisition, and reconnaissance systems equipment and services.

j. **Domain Service –** in active domain services (AD DS), it is a server role in active directory that allows admin to manage and store information about resources from a network, as well as application data, in a distributed database.

k. **End User –** refers to all sailors, marines and employees, guest, and contractors who use computer and other electronic device to access PCG ICT infrastructures and to accomplish assigned task or functions.

l. **Guest Mobile Phone –** personal mobile devices that are installed with either customized applications or confidential, restricted, and unclassified information within the PCG organization, other units, government agencies, and third-party stakeholders.

m. **Guest Network** – a separate non-secured network provided by the PCG to visitors, guest, and end users requiring limited internet access only.

n. **Information infrastructures (infostructures)** – refers to the communications networks and associated information systems that support operational and administrative activities of the PCG.

o. **Information Security Officer** - refers to appointed officer who assists the commanding officer in discharging his responsibilities of safeguarding classified information and material

p. **Infrastructure** – refers to the fundamental facilities and system serving a country, city, or area, including the services and facilities necessary for its economy to function

q. **Internet of things (IoT) Devices** – also something referred to as the Internet of Everything (IoE), consist of all the web-enabled devices that collect, send and act on data they acquire from their surrounding environments using embedded sensors, processors and communication hardware. These devices can interact with humans to get instructions to set them up and access the data, but the devices also generate massive amounts of Internet traffic, including loads of data that can be used to make the devices useful, but can also be mined for other purposes. All this new data, and the Internet accessible nature of the devices, raises both privacy and security concerns. Examples of this device are smart TV, air conditioning unit, refrigerator, electrical plug, locks, light, etc.

r. **PCG Collaboration Suite (PCGCS) -** it is an email platform installed in Network utilized by PCG units/offices for communicating unclassified information to other government agencies and third-party stakeholders.

s. **PCG Messenger System** - is the PCG customized application software developed for chat and file transfer used by PCG units and offices in daily official communications (future development).

t. **PCG RED network -** is described as PCG internet which uses Virtual Private Network (VPN) but at the same time accessible via internet.

u. **Regular Mobile Phone** - PCG issued managed mobile devices that are installed with either customized applications or authorized third party software used for communication and collaboration of confidential, restricted, and unclassified information within the PCG organization, other AFP units, government agencies, and third party stakeholders.

v. **Secured Email System** - it is an email platform installed in PCG Gray Network utilized by PCG units/offices for communicating confidential and restricted information to other AFP units and Uniformed Service.

w. **Secured Mobile Phone -** PCG issued secured and managed mobile devices that are installed with either customized applications or authorized third party software used for communication and collaboration of classified information within the PCG organization.

x. **Supervisory Control and Data Acquisition (SCADA)** – generally refers to vessel computer system that monitors and controls a process. In the case of the transmission and distribution elements not limited to the following systems: Ships Combat System, and Propulsion and Power Monitoring and Control System. SCADA will monitor substances, transformers and other electrical assets. SCADA systems are typically used to control geographically dispersed assets that are often scattered over thousands of square kilometers.

y. **Third Party Stakeholders** – refers to a person or company who may be indirectly involved but is not a principal party to an arrangement, contact, deal, lawsuit, or transaction.

z. **Untrusted Network** – A setting that is not secure and shows evidence of vulnerabilities such as public wifi, and networks other than categorized in this policy.

aa. **Workstations** – are computing devices directly connected to the PCG network/s, owned and managed by the PCG. The term can refer to desktop computers, and laptops.

bb. **Virtual Private Network (VPN)** - is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

V. POLICY:

The Philippine Coast Guard shall ensure the resiliency of its infrastructure and shall provide necessary safeguards to guarantee the confidentiality, integrity, and availability of digital information transmitted in the information infrastructure. It is therefore, the responsibility of the unit commanders to implement security controls in order to insure and maintain credible of the cyber security posture. Hence, the PCG shall adhere to basic function in cybersecurity, which are identify, detect, protect, respond, and recover.

In general, PCG shall implement classification and management of its critical ICT assets in order for the effective and efficient implementation of cybersecurity.

1) Network Management

PCG classifies and categorizes electronic document, computer system and storage media according to its utilization. The PCG shall employ domain services for effective management and administration computers, service and network devices. In order to standardize the development of information network, the PCG information network shall be categorized as closed (Red), Controlled Open Public (Gray), Demilitarized Zone (DMZ), and Guest Networks

a) Closed Network (Red Network)

i. Closed Network shall be properly monitored, protected, hardened, and secured with appropriate security systems and devices;

ii. Secret and CONRES computer and servers shall be connected in this type of network;

iii. Unclassified servers and computer are prohibited to be connected in this type of network;

iv. Top secret computer shall be prohibited to be connected in this type of network;

v. Guest computer are prohibited in this type of network

vi. All PCG mission critical information system shall utilize this type of network

vii. PCG shall develop, implement, secure and maintain email system for exchanging secret information in this type of network;

viii. PCG shall develop, implement, secure, and maintain email system for exchanging CONRES information in this type of network

ix. White listing of application, services, protocols and ports shall be implemented in this type of network;

x. Internet services shall be prohibited in this type of network, however point to point connectivity through internet shall be allowed provided it shall employ secured connectivity thru VPN tunneling;

xi. PCG closed network shall be physically separated from other type of network; and;

xii. Shall employ identification, authentication, authorization, and accountability (IAAA) system for the access to network resources.

b) Controlled Open Public Network (GRAY Network)

i. This type of network shall be properly monitored, protected, hardened, and secured with appropriate security system and devices;

ii. CONRES and Unclassified computer and servers may be connected in this type of network;

iii. Top secret computer shall be prohibited to be connected in this type of network;

iv. PCG shall employ email and collaboration systems for CONRES and unclassified communication;

v. PCG shall implement logical separation of networks;

vi. PCG Shall employ email and collaboration systems for CONRES and classified communications;

vii. PCG controlled open Public network shall be physically separated from the closed network, however it could be logically separated from guest network and demilitarization zone; and;

viii. Shall employ identification, authentication, authorization, and accountability (IAAA) system for the access to network resources.

c) **Demilitarized Zone (DMZ)**

i. This type of network shall be properly monitored, protected, hardened, and secured with appropriate security system and devices;

ii. PCG shall regulate and implement white listing of ports, protocols and services; and;

iii. All public facing service such as email, website, and customized services shall utilized this type of network;

d) **Guest Network**

i. This type of network shall be properly monitored, protected, hardened, and secured with appropriate security systems and devices;

ii. PCG shall regulate and implement white listing of ports, protocols and services;

iii. This type of network shall only be utilized by the guest of third party stakeholder;

iv. All computer not yet configured with baseline configuration shall utilize this type of network; and;

v. Top secret, secret, CONRES, and Unclassified computer are prohibited to be connected in this type of network.

vi. Network access must not exceed to more than three (3) hours;

2) **Computer Management**

PCG computer system shall be managed and configured in accordance to its purpose and use. The PCG shall implement policy that classify, monitor, audit, and secure all computer system in the infrastructure

a) Computer system with Top Secret electronic document shall be classified as Top Secret and shall be tagged as green;

b) Computer system with secret electronic documents shall be classified and shall be tagged with Red;

c) Computer system with confidential and restricted electronic documents shall be classified as confidential/restricted (CONRES) and shall be tagged with Blue;

d) Top secret computer shall be prohibited to be connected to any network;

e) Secret computer shall be connected to close Network;

f) Secret computer shall be prohibited to be connected to Controlled open public network;

g) CONRES computer shall be connected either in closed network or controlled open network;

h) Unclassified computer shall be connected only to controlled open public network;

i) Unclassified computer shall be prohibited to be connected to closed network;

j) Computer system with unclassified electronic documents shall be classified as unclassified and shall tagged with Gray;

k) All computers shall be managed and administered by CGWCEISC;

l) All computers shall be properly configured with baseline configuration prior issuance to the end-user

m) All servers shall be configured with baseline configuration prior its deployment;

n). Baseline configuration shall be determined, configured, and implementation by CGWCEISC only;

o) CGWCEISC shall employ identification, authentication, authorization, and accountability (IAAA) system for the access to network resources;

p) All servers and computer shall be employed with protocol and services white listing;

q) Servers and computer shall be monitored, accounted, configured, and administered property and securely; and;

r) Servicing of servers and computers outside of PCG premises shall be prohibited unless authorized by Unit commanders

s) Usage of counterfeit software or Operating System is prohibited

t) All computers must undergo cleaning procedure prior connecting to the network

3) Storage Management

PCG storage system shall be managed and configured in accordance to its purpose and use. The PCG shall implement policy that classify, monitory, audit, network, and secure all storage system in the infrastructure.

a) Storage system stored with top secrete electronic documents shall be classified as top secret and tagged with Green;

b) Top Secret storage system shall be prohibited to be connected to any networks or to a computer system other than top secret;

c) Storage system stored with secret electronic documents shall be classified as secret and tagged with Red;

d) Secret storage system shall be connected to closed network;

e) Secret storage system shall be prohibited to connect to controlled Open Public Network;

f) Storage system storage with confidential/Restricted electronics document shall be classified as CONRES and tagged with Blue;

g) CONRES storage system shall be connected to closed and controlled open public networks;

h) Remote access to the CONRES storage system shall employ encryption protocols such as VPN tunneling;

i) Storage system stored with Unclassifie electronic documents shall be classified as unclassified and tagged with Gray;

j) Unclassified storage system shall be connected to controlled open public network;

k) Unclassified storage system shall be prohibited to be connected to closed network;

l) Network storage shall be the primarily media for storing electronic documents and it shall be properly secured and managed;

m) Network storage shall be managed and administered by CGWCEISC;

n) Network storage Back-up shall be conducted regularly;

o) Files and folder stored at network devices shall be shared to specific office and on need to know basis;

p) Top secret and CONRES computer shall prohibited the utilization of portable storage devices;

q) Secret documents shall be stored in secret network storage installed at PCG closed network;

r) Unclassified computer shall regulate the utilization of portable storage devices; and;

s) File extension white listing and storage quota shall be implemented;

t) Storage system must be protected by Anti-Malware and Anti-Virus service/s or any equivalent security protection.

4) Bring Your Own Devices (BYOD)

PCG shall implement security controls to the BYODs to maintain the confidentiality, integrity and availability of information stored in it;

a) All BYOD shall be regulated and registered, monitored, accounted and audited;

b) BYOD devices connected to PCG infrastructure that utilizes its services shall employ utmost security;

c) PCG shall employ mobile device management system;

d) BYOD shall maintain secure access to PCG infrastructure;

e) BYOD shall maintain visibility in the PCG networks;

f) BYOD shall be prohibited to be connected to closed network;

g) BYOD owners shall adhere to the PCG usage policies;

h) BYOD owner shall take full responsibility for the protection of their own device; and;

i) Intentional/Unintentional introduction of malware that may result to security breach caused by BYOD will constitute a punishable act under existing Philippine laws

j) All devices from end user shall undergo scanning prior connecting to the PCG network

/10

5) **Internet of Things Device (IoT) Device**

a) All IoT shall be regulated, registered, monitored, accounted and audited;

b) PCG shall employ protection system to all IoT devices;

c) IoT devices firmware/operating system shall be regularly updated;

d) IoT shall be prohibited to be connected to PCG closed network;

e) PCG shall implement policy control that disable unwanted features;

f) PCG shall implement managed access to IoT data ;

g) PCG shall implement appropriate protection for all potential attack surface

h) PCG shall implement secure connectivity and encrypted data transmission

i) PCG shall restrict access to or control of the devices;

j) Owner of the IoT device shall take responsibility for the protection of their own device; and;

k) Intentional/Unintentional introduction of malware that resulted to security breach to PCG network through IoT constitute a Punishable act under existing Philippine laws.

6) **Mobile Phone Management (Future Development)**

a) Mobile phones issued to all PCG Units/Offices shall be managed and secure according to the following;

1) **Secured Mobile Phone**

i) Shall be issued to all PCG Units/Offices for communicating and collaborating classified (top secret/secret/confidential/restricted) information;

ii) Shall be used for communication and collaboration within the PCG. It shall be connected to PCG closed network through a secured connectivity by employing tunneling technology such as VPN;

iii) Internet use such as browsing and downloading of mobile applications shall be prohibited however, internet shall be used only as a medium of secured connectivity to PCG closed network via VPN tunneling

iv) Shall be installed with PCG customized application for mobile device and/or authorized third party mobile applications for voice and data communication;

v) Shall be manage by mobile management system installed at the PCG closed network and shall be accounted, audited, managed, and secured by PCGICT Personnel;

vi) Shall be employed with multi-factor authenticate system and all files and phonebooks can be remotely destructed/erased /formatted if the device will be lost; and;

vii) Shall be tagged as RED mobile device thru customized sticker and/or mobile background.

`2) Regular Mobile Phone

i) Shall be issued to all PCG Units/Offices for communicating and collaborating confidential, restricted and unclassified information; but not limited to coordination, monitoring, queries, assistance and rendering support to maritime stakeholders.

ii) Shall be used for communication and collaboration within the PCG, other AFP units, government agencies, and third party stakeholders. It shall be connected to PCG controlled Open Public Network however, it shall be managed through a mobile management system deployed in PCG Gray network;

iii) Shall be installed with PCG customized application for mobile devices and/or authorized third party mobile application for voice and data communication;

iv) Shall be accounted, audited, managed, and secured by PCGICT personnel. It shall be employed with multi-factor authentication system and all files and phonebooks can be remotely destructed/erased/formatted if the device will be lost, and,

v) Shall be tagged as GRAY mobile device thru customized sticker and/or mobile background.

3) Guest Mobile Phone

i. Shall only be allowed to be connected to the guest network and shall be monitored when connected to the PCG Gray network; and,

ii. Shall only be allowed to access Internet services however, shall be prohibited from accessing other network services.

a) Secure and Regular Mobile devices shall properly configured with baseline configuration prior issuance to the end-user;

b) Mobile devices shall be monitored, accounted, configured, and administered properly and securely;

c) PCG shall employ Mobile Management System to effectively secure and manage all PCG issued mobile devices;

d) Classified information shall not be stored in mobile devices; and,

e) PCG shall ensure the proper disposal of mobile devices issued to PCG personnel.

7) SCADA SYSTEMS

a) PCG shall implement security controls for the SCADA Systems (Ships' Combat System, Propulsion Advance Bridge Management System, Mission management System and Power Monitoring and Control System) to maintain the confidentiality, integrity and availability of information stored in it;

b) All SCADA Systems shall be regulated, registered, monitored, accounted and audited;

c) PCG shall employ protection system to all SCADA Systems devices;

d) The mobile storage devices (USB flash Disk or External Hard Disk Drive) shall be prohibited from attaching to Computing devices in SCADA Systems unless authorized by the Unit Commander as necessary for the operation and upgrade of the system; and,

e) The SCADA Systems shall be physically separated from any networks.

8) Printers, Scanners, and Photocopying Machines

a) Printers, scanners, and photocopying machine shall be classified in accordance to the Computer Systems and networks attached to it;

b) Network printers and photocopying machines shall be monitored, audited, and secured properly;

c) Photocopying machines that store information shall properly checked and monitored;

d) All data stored in the rented photocopying machine shall be deleted/shredded;

e) Firmware updated shall be implemented to all printers, scanners and photocopying machines; and,

ßp

f) All printers, scanners, and photocopying machines shall be regulated, registered, monitored, accounted and audited.

9) Electronic Documents Management

Official electronic documents that reside in computer system, and stored in storage devices in the PCG network require protection. The electronic documents shall be categorized as Classified and Unclassified as provided in the PCG Regulations G200 – 001, ("Security of Classified Matters"). Classified documents are categorized as Top Secret, Secret, Confidential, and Restricted. PCG shall implement the following security controls to secure its electronic documents:

a) Top Secret shall be drafted in a computer system categorized as Top Secret;

b) Top Secret electronic documents shall be transmitted via courier as prescribed by existing policy on Security of Classified Matters;

c) Top Secret electronic documents shall be stored in an encrypted and isolated network or in a storage device employed with the highest encryption standards and physical security (e.g. vault);

d) Secret documents shall be drafted in a computer system categorized as Secret;

e) Secret electronic documents shall be transmitted over PCG Closed Network;

f) Secret electronic documents shall be stored in a storage device either it is networked or through removable storage and shall be employed with the highest encryption standard;

g) Secret electronic document shall be communicated through Red Network Email System or PCG Messenger System only;

h) Confidential documents shall be drafted in a computer system categorized as Confidential/Restricted (CONRES);

i) Confidential electronic documents shall be transmitted on both Closed and Controlled Open Public Network;

j) Confidential electronic document shall be stored in a storage device either networked or through removable storage and shall be employed with encryption;

k) Confidential electronic document shall be communicated either on Secured Email System or PCG Messenger System in Gray Network or Email System or PCG Messenger System in Red Network;

l) Restricted electronic documents shall be drafted in a computer system categorized as CONRES;

m) Restricted electronic documents shall be transmitted on both Closed and Controlled Open Public Network;

n) Restricted electronic documents shall be stored in a storage device either networked or through removable storage and shall be employed with encryption;

o) Restricted electronic document shall be communicated either on Secured Email System or PCG Messenger System in Gray Network or Email System or PCG Messenger System in Red Network;

p) Unclassified documents shall be drafted in a computer system categorized as Unclassified;

q) Unclassified electronic documents shall be transmitted on both Closed and Controlled Open Public Network;

r) Unclassified electronic documents shall be stored in a storage device either networked or through removable storage and do not need employment of encryption;

s) Philippine Coast Guard Collaboration Suite shall be used to communicate unclassified electronic documents with other government agencies, and commercial sectors;

t) Access to classified electronic documents shall be prohibited over un-trusted network;

u) Remote access of CONRES electronic documents shall employ appropriate security schemes such as Virtual Private Network (VPN; and,

v) All electronic document shall have an onsite and offsite backup and recovery system,

VI. GENERAL GUIDANCE

The following are general guidelines to ensure the cybersecurity posture of the PCG and maintaining information assurance in the PCG infrastructure. These guidelines were intentionally accepted cybersecurity standards published by the National Institute of Standard and Technologies (NIST) to address compliance of all layers of cybersecurity spectrum.

a) Asset Management

The data personnel, devices, system, and facilities that enable the PCG to achieve operation purposes are identified and manage consistent with their relative important to PCG objectives and the organization's risk strategy. The PCG shall develop and implement following controls;

1) The PCG shall employ a system or means for an automated asset management where inventory of physical devices connected into the network can be monitored.

2) The PCG shall conduct regular inventory of all physical devices and systems;

3) The PCG shall conduct regular inventory of all software platforms and applications;

4) The PCG shall map network, communication and data flow;

5) The PCG shall audit all external and internal information system;

6) The PCG ICT resources shall be prioritized based on their classification, critically, and operational and administrative value; and;

7) The PCG shall establish cybersecurity roles responsibilities for the entire workforce and third-party stakeholders.

b) Operational and administrative Environment

The organization's mission, objective stakeholders, and activities should be understood and prioritized, and risk management decisions. Hence, PCG shall implement the following control;

1) The PCG shall identify and communicate the organization's role in the operation:

2) The PCG shall identify and communicate the organization's place in critical infrastructure and in the government sector;

3) The PCG shall establish and communicate the priorities for organizational mission, objectives, and activities;

4) The PCG shall establish dependencies and critical functions for delivery of critical service; and;

5) The PCG shall establish resilience requirements to support delivery of critical service

c) Governance

The policies, procedures, and processes to manage and monitor the organization`s regulatory, legal, risk, environmental, and operational requirements shall be understood and shall inform the management of cyber security risk. Hence, the PCG shall implement the following controls;

1) Organizational cyber security related policy shall be established;

2) Information security roles & responsibility shall be coordinated and aligned with internal roles and external partners;

3) Legal and regulatory requirement regarding cybersecurity, including privacy and civil liberties obligations, shall be understood and managed; and;

4) Governance and risk management processes shall address cybersecurity risk.

d). Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, function, image, or reputation), organizational assets, and individuals. Hence, the PCG shall implement the following controls;

1) The PCG shall conduct Cyber Risk Assessment (CRA) to determine the gap between industry standards and current unit cybersecurity posture.

2) The PCG shall adopt the NIST 20 Critical Security Controls as mentioned in the PCG cyber warfare Doctrine as the de facto yardstick by which the cybersecurity posture of a unit can be measured

3) The result of the CRA shall be the unit's basis for programming C4IS requirements;

4) The PCG shall identify asset vulnerabilities and property document it;

5) The PCG shall engage with local and international partners to maintain threat and vulnerability information through information sharing forums and sources;

6) All threats, boat internal and external, are identified and documented;

7) Potential operational and administrative impacts and likelihoods shall be promptly and properly identified;

8) Threats, vulnerabilities, likelihoods, and impacts shall be used to determine risk; and,

9) Risk responses shall be identified and prioritized.

e). Risk Management Strategy

The organization's priorities, constraints, risk tolerances, and assumptions shall be established and used to support operational risk decisions. Hence, the PCG shall implement the following controls:

1) Risk management processes shall be established, managed, and agreed to by organizational stakeholders;

2) Organizational risk tolerance shall be determined and clearly expressed; and;

3) The organization's determination of risk tolerance shall be informed by its role in critical infrastructure and sector specific risk analysis.

f). Access Control

Access to assets and associated facilities is limited to authorized users, processes, device and to authorized activities and transactions. Hence, the PCG shall implement the following controls:

1) Identities and credentials shall be managed for authorized devices and users;

2) Physical access to assets shall be managed and protected;

3) Remote access shall be managed;

4) Access permission shall be managed and incorporating the principles of least privilege and separation of duties; and,

5) Network integrity shall be protected, incorporating network segregation where appropriate.

g). Awareness and Training

The organization`s personnel and partners shall be provided cybersecurity awareness education and shall be adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. Hence, the PCG shall implement the following controls:

1) All PCG personnel shall be cybersecurity aware and trained;

2) All privileged users should understand their respective roles and responsibilities;

3) Third-party stakeholders (e.g., suppliers, customers, partners) should understand their respective role and responsibilities;

4) Staff and Unit Commanders shall understand roles and responsibilities;

5) Physical and information security personnel should understand their respective roles and responsibilities; and,

6) The conduct of annual cybersecurity month, cyber defense exercise, and related activities shall be encouraged.

h). Data Security

Information and records (data) shall be managed consistent with the PCG risk strategy to protect the confidentiality, integrity, and availability of information. Hence, the PCG shall implement the following controls:

1) Data at rest shall be protected;

2) Data-in-transit shall be protected;

3) Assets shall formally be managed throughout removal, transfers, and disposition;

4) Adequate means to ensure confidentially, integrity, and availability of information shall be maintained;

5) Protections against data leaks shall be implemented;

6) Integrity checking mechanisms shall be used to verify software, firmware, and information integrity; and

7) The development and testing environment shall be separated from the production environment.

i). Information Protection Processes and Procedures

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures shall be maintained and used to manage protection of information systems and assets. Hence, the PCG shall implement the following controls;

1) Baseline configuration of information technology/industrial management system shall be created and maintained;

2) System development life cycle to manage systems shall be implemented;

3) Configuration change control processes shall be in place;

4) Backups and information shall be conducted, maintained, and tested periodically;

5) Policy and regulations regarding to physical operating environment for organizational assets shall be met;

6) Data shall be destroyed according to policy;

7) Protection processes shall be continuously improved;

8) Effectiveness of protection technologies shall be shared with appropriate parties;

9) Response plans (Incident Response and Business Continuity) and recovery plans (Incident Response and Disaster Continuity) shall be in place and managed;

10) Response and recovery plans shall be tested;

11) Cybersecurity shall be included in human resources practices (e.g., de-provisioning, personnel screening); and,

12) A vulnerable management plan shall be developed and implemented.

j). Maintenance

Maintenance and repairs of information system components shall be performed consistent with policies and procedures. Hence, the PCG shall implement the following controls:

1) Maintenance and repair of organizational assets shall be performed and logged in a timely manner, with approved and controlled tools; and,

2) Remote maintenance of PCG ICT assets shall be approved, logged, and performed in a manner that prevents unauthorized access.

k). Protective Technology

Technology security solutions shall be managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Hence, the PCG shall implement the following controls:

1) Audit/log records shall be determined, documented, implemented, and reviewed in accordance with policy;

2) Removable media shall be protected and its use restricted according to procedures and guidelines;

3) Access to systems and assets shall be controlled, incorporating the principle of least functionality; and;

4) Communications and control network shall be protected.

l). Anomalies and Events

Anomalous activity shall be detected in a timely manner and the potential impact of events shall be understood. Hence, the PCG shall implement the following controls:

1) A baseline of network operations and expected data flows for users and systems shall be established and managed;

2) Detected events shall be analyzed to understand attack targets and methods;

3) Event data shall be aggregated and correlated from multiple sources and sensors;

4) Impact of events shall be determined; and,

5) Incident alert thresholds shall be established.

m). Security Continuous Monitoring

The information system and assets shall be monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Hence, the PCG shall implement the following controls:

1) PCG information network shall be monitored to detect potential cybersecurity events;

2) The physical activity shall be monitored to detect potential cybersecurity events;

3) Personnel activity shall be monitored to detect potential cybersecurity events;

4) Malicious code shall be detected;

5) Unauthorized mobile code shall be detected;
6) External service provider activity shall be monitored to detect potential cybersecurity events;

7) Monitoring for unauthorized personnel, connections, devices, and software shall be performed; and,

8) Vulnerability scans shall be performed.

n). Detection Processes

Detection processes and procedures shall be maintained and tested to ensure timely and adequate awareness of anomalous events. Hence, the PCG shall implement the following controls:

1) Roles and responsibilities for detection shall be well defined to ensure accountability;

2) Detection activities comply with all applicable requirements;

3) Detection processes shall be tested;

4) Event detection information shall be communicated to appropriate parties; and,

5) Detection processes shall be continuously improved

o). Response Planning

Response processes and procedures shall be executed and maintained to ensure timely response to detected cybersecurity events. Hence, there will be a separate SOP for the PCG computer emergency team (PCG CERT).

p). Response Communication

Response activities shall be coordinated with internet and external stakeholders, as appropriate, to include external support law enforcement agencies. Hence, the PCG shall implemented the following controls:

1) Personnel should know their roles and order of operations when a response is needed;

2) Events shall be reported consistent with established procedures and guidelines;

3) Information shall be shared consistent with response plans;

4) Coordination with stakeholders shall occur consistent with response plans; and,

5) Voluntary information sharing shall occur with external stakeholders to achieve broader cybersecurity situational awareness.

q). Analysis

Analysis shall be conducted to ensure adequate response and support recovery activities. Hence, the PCG shall implement the following controls:

1) Notifications from detection systems shall be investigated;

2) The impact of the incident should be understood;

3) Forensics shall be performed; and,

4) Incidents shall be categorized consistent with response plans.

r). Mitigation

Activities shall be performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. Hence, the PCG shall implement the following:

1) Incidents shall be contained;

2) Incidents shall be mitigated; and,

3) Newly identified vulnerabilities shall be mitigated or documented as accepted risks.

s). Response Improvements

The PCG organizational response activities shall be improved by incorporating lessons learned from current and previous detection/response activities. Hence, the PCG shall implement the following controls:

1) Response plans shall incorporate lessons learned; and,

2) Response strategies shall regularly updated.

t). Business Continuity and Recovery Planning

Recovery processes and procedures shall be executed and maintained to ensure timely restoration and continuity of systems or assets affected by cybersecurity events. Hence, PCG shall execute recovery plan during or after an event. Hence, PCG shall execute recovery plan during or after an event.

u). Recovery Improvements

Recovery planning and processes shall be improved by incorporating lessons learned into future activities. Hence, the PCG shall implement the following controls:

1) Recovery plans shall incorporate lessons learned; and,
2) Recovery strategies shall be updated.

v). Recovery Communications

Restoration activities shall be coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. Hence, the PCG shall implement the following controls:

1) Public relations shall be managed;

2) Reputation after an event shall be repaired; and,

3) Recovery activities shall be communicated to internal stakeholders and executive and management teams.

VII. RESPONSIBILITIES:

a. Head of Offices and Commanders/Operational/Support Command and Units

1) Ensure all PCG personnel, civilian employees, Third Party Stakeholders, and guests adhere to the provisions of this policy;

2) Develop appropriate procedures on the operation ensure implementation of this policy;

3) Designate Document Security Officer;

4) Develop procedures and guidelines on the operations of systems implemented in this policy;

5) Coordinate with the DCS for MCWEIS, CG-11 on the formulation and review of this policy and other relevant cyber security policies;

6) Plan and program all activities pertaining to the implantation of this policy in the APB; and,

7) Investigate and recommend appropriate punishment on the violation of this policy.

b. Coast Guard Weapons, Communication, Electronics and Information System Command (CGWCEISC)

1) Tagging of the computers and establish procedures and guidelines for base-lining and white listing;

2) Develop plans, designs, milestone, and technical requirements of this policy to the PCG Cybersecurity Plan;

3) Develop plans, designs and technical and budgetary requirements of this policy to the Information System Strategic Plan;

4) Formulate appropriate procedures and guidelines on the installation, configuration, administration, and maintenance of all systems implemented in this policy; and,

5) UPR for the implementation and enforcement of this policy

c. Deputy Chief of Coast Guard Staff for Maritime Communication, Weapons, Electronics and Information System, CG-11

1) Ensure all PCG Personnel, civilian employees, and Third party stakeholders adhere to the provisions of this policy;

2) SPR for the supervision and monitoring of the implementation and enforcement of this policy;

3) Conduct annual inspection on PCG units compliance to this policy;

4) Conduct a regular review of this policy.

d. Deputy Chief of Coast Guard Staff for Intelligence, Security, and Law Enforcement, CG-2

1) Ensure all PCG personnel. civilian employees, and Third Party Stakeholder adhere to the provisions of the policy;

2) SPR for the conduct background investigation of the Third Party Stakeholders; and,

3) Coordinate with the DCS for MCWEIS, CG-11 on the formulation and view of this policy and other relevant cyber security policies.

e. The PCG Legal Service

1) Review and evaluate the legal context of this policy and other relevant cyber security policies in ensuring compliance to laws, statutory, and regulation; and,

2) Recommend sanctions to erring personnel based on existing national cyber-related laws.

VIII. ADMINISTRATIVE SANCTIONS:

PCG personnel and third party contractors who are found deliberately violating this policy shall be dealt with accordingly. Appropriate filing of case shall be pursued against individuals or those that contribute to the defilement or sabotage of PCG infostructure.

IX. EFFECTIVITY: This circular shall take effect upon publication

BY COMMAND OF ADM HERMOGINO PCG:

EDUARDO D FABRICANTE
COMMO PCG
Chief of Coast Guard Staff

OFFICIAL:

LIEZEL B BAUTISTA
CDR PCG 18 JUN 2019
Coast Guard Adjutant