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

**NHQ-PCG/CG-11** 10 October 2025

**STANDING OPERATING PROCEDURE**
**NUMBER 14-25**

## BASELINE CONFIGURATION OF PCG FIREWALLS

### 1. REFERENCES

A. National Cybersecurity Plan 2023-2028;

B. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 dated 26 February 2024;

C. NHQ-PCG/CGWCEISC/CG-11 Circular No. 03-25, entitled "Philippine Coast Guard Cybersecurity Framework" dated 08 January 2025; and

D. NHQ-PCG/CG-11 Circular No. 11-19, entitled "Philippine Coast Guard Cybersecurity Policy" dated 07 October 2019.

### 2. GENERAL

The Commandant, PCG has emphasized the need to strengthen PCG cybersecurity to protect its network infrastructure, especially as the Organization becomes increasingly reliant on information and communication technology. In response, various initiatives have been implemented, including cybersecurity awareness seminars and the issuance of policies and directives.

In order to further enhance the cybersecurity posture of the Command, standardized baseline for firewall configuration and uniform web filtering rules shall be established to ensure a consistent and robust defense against potential cyber risks across all PCG Units.

### 3. PURPOSE

This SOP provides for the implementation of the baseline firewall configuration and web filtering rules that shall be enforced in the PCG firewalls in order to enhance the network security of the PCG.

## 4. SCOPE

This directive applies to the following:

A. All personnel accessing the services at the PCG Local Area Network;

B. Guests who are given authorized access to internet services at the PCG's Guest Network; and

C. All firewalls of the Command.

## 5. DEFINITION OF TERMS

A. **Blacklisted Websites** – a list of URLs flagged as potentially hazardous and harmful.

B. **Firewall** – a hardware or software-base security system that regulates incoming and outgoing network traffic based on predetermined security rules, and acts as a barrier against unauthorized access.

C. **Privileged users** – individuals authorized to access critical IT systems and perform tasks that standard users are not permitted to execute.

D. **Web-filtering rules** – a set of security policies that restrict access to specific websites or web content to improve internet security and limit access to unproductive or inappropriate material.

E. **Whitelisted Websites** – list of allowed URLs deemed safe and trustworthy, permitted for access within the network.

## 6. OBJECTIVES

A. Implement standard web filtering rules on PCG Unit firewalls with website or URL filtering capabilities.

B. Reduce the attack surface of the PCG Information Infrastructure by blocking unauthorized websites or specific website categories.

C. Enhance the PCG's cybersecurity posture through centralized network security monitoring; and

D. Ensure that the limited Internet Bandwidth Resources are used only for official functions/activities of the Command.

## 7. POLICIES

To ensure the standardization of the firewall rules implementation, the following are the policies:

A. All PCG personnel shall adhere to the provisions of this directive;

B. All PCG Units, under the guidance of CGWCEISC, shall install firewalls in respective Units;

C. CGWCEISC shall be the only authorized network administrator responsible for configuring firewalls for the PCG. They shall ensure that baseline web filtering rules and categories are implemented based on the grouping in **Annex A**;

D. All devices that need to connect to the network shall be registered in the firewall. The network administrator shall establish and maintain an inventory including ownership of all devices;

E. CGWCEISC shall monitor weekly and monthly incidents and threats to the information infrastructure and take appropriate mitigation measures;

F. Request for major changes to the firewall rules shall be addressed to O/CG-11 thru CGWCEISC.

G. Privileged users shall be the Officers and key personnel who are allowed to use selected services and whom request are needed in the performance of their duties. The Unit/Office 11s or WCEIS Officers shall maintain a regularly updated list of privileged users for monitoring and management;

H. PCG personnel requesting inclusion on the list of privileged users shall file a request to their Unit/Office 11s or WCEIS Officers for endorsement and subsequent approval of the Head of Unit/Office;

I. Unit/Offices 11s shall forward the implementation details of privileged user inclusion to the respective CGWEIS Regional Center, which shall maintain an updated list for proper inventory, monitoring and management; and

J. CGWCEISC shall submit Network Security Report to the Commandant, PCG (Attn: CG-11) every 25th of the month, semi-annual and annual.

## 8. PROCEDURES

A. The web filtering rules shall be applied to all firewalls, including on-premises and cloud-based, installed across all PCG Units.

B. Before implementation, all necessary equipment, documentation and references must be prepared. This includes compiling a list of whitelisted and blacklisted websites and online applications categorized in **Annex A**, as well as developing a baseline firewall configuration covering access control, protocol blacklisting and whitelisting, rules, categories, services and ports.

C. Once preparations are complete, configuration and testing will follow. This involves applying the approved list of whitelisted and blacklisted websites or online applications to the firewall.

D. Following testing, an initial Troop Information and Education (TI&E) session shall be conducted for PCG personnel to ensure awareness and compliance with this policy, with periodic sessions scheduled as needed. TI&E shall also be conducted whenever firewall rules updates are recommended.

E. Any changes in firewall configuration, including updates, rule additions or removals, must be properly documented with details such as the date, time, nature of the change, and the personnel responsible.

F. Secure backup of firewall configuration must be established and maintained to ensure quick restoration in the event of system failure, corruption or compromise.

## 9. RESPONSIBILITY

### A. Commander, Coast Guard Weapons, Communications, Electronics and Information Systems Command (CGWCEISC)

i. Unit with primary responsibility for the implementation of this SOP;

ii. In coordination with CG-11, provide SME in the conduct of TI&E on this directive and on the update of this SOP;

iii. Ensure rules in **Annex A** are configured and implemented in the firewalls;

iv. Ensure and maintain an updated list of privilege users; and

v. Submit PCG Network Security Report to the Commandant, PCG, (Attn: CG-11) every 25th day of the month, semi-annual and annual.

vi. Shall inform Units/Offices' CGWCEISC personnel all detected suspicious or malicious IP addresses or URLs to be promptly entered into the firewall to prevent unauthorized access or attacks.

vii. During the installation of the firewalls, subject matter experts (SMEs), preferably from CGWCEISC, shall conduct a lecture or information drive for PCG personnel assigned to Information Technology within the concerned Commands, Services, Units or Offices. Said activity shall ensure that designated personnel are adequately equipped to perform basic troubleshooting procedures in the event of hacking attempts or system infiltration by hostile entities.

viii. Shall conduct quarterly firewall audits to remove outdated rules and maintain alignment with evolving security standards.

**B. Commander, Functional Commands / Coast Guard Districts / Admin Support Commands / Operational Support Commands / Special Service Commands**

i. Ensure compliance with this SOP;

ii. In coordination with CGWCEISC, conduct TI&E to Officers, Enlisted Personnel and NUP on the policy, and henceforth every update on the rules of the firewalls; and

iii. Ensure and maintain an updated list of privileged users.

**C. Deputy Chief of Coast Guard Staff for Maritime Communications, Weapons, Electronics and Information System, CG-11**

i. SPR for the implementation of this SOP;

ii. Conduct review and assessment on the monthly PCG Network Security report; and

iii. Based on the assessment on the monthly report, issue cybersecurity-related policy and guidance.

**D. Deputy Chief of Coast Guard Staff for Intelligence, CG-2**

i. Assist CG-11 on the review and assessment of the PCG Network Security report submitted by CGWCEISC; and

ii. Ensure attendance of personnel in the conduct of TI&E.

## 10. EFFECTIVITY

The provision of this SOP shall take effect upon publication.

**BY COMMAND OF ADMIRAL GAVAN PCG:**

**GLIDE GENE MARY G SONTILLANOSA**
**COMMO PCG**
Acting Chief of Coast Guard Staff

**OFFICIAL:**

**JAYSIEBELL B FERRER**
p **CDR PCG**
Coast Guard Adjutant

*Annex:*
*A – Baseline Configuration for Web Filtering*

ANNEX A

## Baseline Configuration for Web Filtering

| WEB FILTER | GUESTS NETWORK | GENERAL PRODUCTION | STUDENTS OF TRAINING CENTERS | PRIVILEGED USERS |
|---|---|---|---|---|
| Potential Liable | | | | |
| Drug abuse | block | block | block | block |
| Hacking | block | block | block | block |
| Illegal or Unethical | block | block | block | monitor |
| Discrimination | block | block | block | block |
| Explicit Violence | block | block | block | block |
| Extremist Group | block | block | block | monitor |
| Proxy Avoidance | block | block | block | block |
| Plagiarism | block | block | block | block |
| Child Abused | block | block | block | block |
| Adult/Mature Content | | | | |
| Alternative Belief | block | block | block | monitor |
| Abortion | block | block | block | monitor |
| Advocacy Organization | block | block | block | monitor |
| Gambling | block | block | block | monitor |
| Nudity and Risque | block | block | block | block |
| Pornography | block | block | block | block |
| Dating | block | block | block | monitor |
| Weapon (sales) | allow | allow | allow | allow |

| | | | | |
|---|---|---|---|---|
| Drugs | block | block | block | block |
| Sex Education | block | block | block | block |
| Bandwidth Consuming | | | | |
| Freeware and Software Downloads | block | monitor | monitor | monitor |
| File Sharing and Storage | block | block | block | block |
| Streaming Media and Download | block | block | monitor | monitor |
| Peer to Peer Sharing | block | block | block | monitor |
| Online Meeting | allow | allow | allow | allow |
| Security Risk | | | | |
| Malicious Websites | block | block | block | block |
| Phishing | block | block | block | block |
| Spam URLs | block | block | block | block |
| Dynamic DNS | block | block | block | block |
| General Interest – Personal | | | | |
| Advertising | block | block | block | monitor |
| Brokerage and Trading | allow | allow | allow | allow |
| Online Games | block | block | block | block |
| Commercial Web-Based | allow | allow | allow | allow |
| Entertainment | block | block | block | allow |
| Art and Culture | allow | allow | allow | allow |

| | | | | |
|---|---|---|---|---|
| Education | allow | allow | allow | allow |
| Health and Wellness | allow | allow | allow | allow |
| Job Search | allow | allow | allow | allow |
| Medicine | allow | allow | allow | allow |
| News and Media | allow | allow | allow | allow |
| Social Networking | block | block | block | monitor |
| Political Organization | allow | allow | allow | allow |
| Reference | allow | allow | allow | allow |
| Global Religion | allow | allow | allow | allow |
| Shopping | monitor | monitor | monitor | monitor |
| Society and Lifestyles | allow | allow | allow | allow |
| Travel | allow | allow | allow | allow |
| Dynamic Content | allow | allow | allow | allow |
| Web Chat | monitor | monitor | monitor | monitor |
| Instant Messaging | monitor | monitor | monitor | monitor |
| Child Education | allow | allow | allow | allow |
| Real Estate | allow | allow | allow | allow |
| Personal Website and Blog | block | block | block | monitor |
| Content Server | allow | allow | allow | allow |
| Auction | allow | allow | allow | allow |

| General Interest – Business | | | | |
|---|---|---|---|---|
| Finance and Benefit | allow | allow | allow | allow |
| Search Engines and Portals | allow | allow | allow | allow |
| General Organizations | allow | allow | allow | allow |
| Government and Legal Organization | allow | allow | allow | allow |
| Information Technology | allow | allow | allow | allow |
| Web Hosting | allow | allow | allow | allow |
| Secure Websites | allow | allow | allow | allow |
| Web-based Application | allow | allow | allow | allow |
| Charitable Organization | allow | allow | allow | allow |
| Remote Access | block | block | block | monitor |

*Legend:*

*Allow* — *authorized access within the PCG network*
*Block* — *unauthorized and cannot be accessed*
*Monitor* — *allowed, but traffic will be monitored by Firewall Administrator*