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

05 March 2019

NHQ-PCG/CG-11

STANDING OPERATING PROCEDURES
NUMBER 05-19

UTILIZATION OF PCG PROVIDED EMAIL SERVICES

I. REFERENCE:

a. HPN SOP NR 14 dtd 08 APRIL 2009 – Utilization of Coast Guard Provided Email Services

b. DICT MC No 2015 002 – Prescribing the Gov Mail Service Guidelines for Phils Gov't Agencies – 27 April 2015

c. DICT Department Circular No 2017 002 – Prescribing the Phils Gov't Cloud First Policy – 18 January 2017

d. RA – 10173 – Data Privacy Act of 2012 – 15 July 2012

e. RA – 10175 – Cybercrime Prevention Act of 2012 – 25 July 2011

f. HPCG Circular No 09-14 – Policy Guidelines to Raise Security, Awareness, Consciousness and Discipline on the use of Information & Communications Technology (ICT) Devices and the Internet of PCG Personnel – 01 September 2014

II. PURPOSE:

This SOP prescribes guidance for the management and proper utilization of the Philippine Coast Guard (PCG) electronic facilities and resources.

III. SCOPE:

This policy applies to the usage and application of the electronic mail system and services provided by the Philippine Coast Guard (PCG) and hosted at

coastguard.gov.ph. Provisions indicated herein apply only to electronic mail in its electronic form. It does not apply to printed copies of electronic mail.

IV. DEFINITION OF TERMS:

a. **Compelling Circumstances** – Circumstances where failure to act may result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of policies, or has a significant effect to National security and conduct of Coast Guard's operations.

b. **Emergency Circumstances** – Circumstances where time is of the essence and where there is a high probability that delaying action would almost certainly result in compelling circumstances.

c. **PCG E-mail System or Services** – The messaging system hosted on coastguard.gov.ph that depends on PCG computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records for purposes of asynchronous communication across computer network system between, among or from PCG personnel.

d. **PCG IT Resources** - Electronic and communications equipment, software, and systems applications including but not limited to computers, computer networks, and applications such as the internet and e-mail.

e. **Substantiated Reason** – Reliable evidence indicating that violation of law or policies listed herein probably has occurred, as distinguished from rumour, gossip, or other unreliable evidence.

f. **System Administrator** – Coast Guard Information System personnel responsible for the upkeep, configuration, and reliable operation of E-mail system.

g. **Time-dependent and Critical Operational Circumstances** – Circumstances where failure to act could seriously hamper the ability of the PCG to conduct operations.

h. **User account and password** – Services provided by the PCG e-mail system to control access to PCG data resources based on an individual personnel's need to access specific data.

V. BACKGROUND:

a. The Philippine Coast Guard provides a communications network capable of providing electronic (E-mail) service, where applicable, to assist in and facilitate legitimate communications. The PCG's network and systems are dedicated to providing service to the public and use of official business.

b. Electronic mail is an integral part of PCG communications. it is the policy of the PCG to encourage the responsible use of electronic mail whether internally or externally generated or viewed. the primary purpose of the PCG electronic mail system is to facilitate the timely and efficient coordination and communication.

c. The PCG's treats all information transmitted through or stored in the system, including E-mail message, as official information. Personnel using the PCG e-mail resources have no expectation of privacy in their use. Coast Guard Weapons Communications, Electronics and Information System Command (CGWCEISC) has the capability and, within the authority listed in this publication, to access, review, and copy, modify, and delete any or all of such information.

d. Files containing personal information of any employee as a result of the employee making incidental use for personal purposes, including transmission of personal E-mail messages will be treated no differently than other business files and information. Accordingly, employees should not use the computer system to send, receive or store any information that they wish to keep private.

VI. POLICIES:

a. Account

1) All active PCG officers, enlisted personnel, and casual civilian employees are required to have PCG E-mail accounts.

2) Accounts not used within a period of three months will be automatically terminated.

3) Accounts of personnel who retired or reassigned from the service will be automatically terminated.

4) Accounts of personnel who are dishonourably discharged from the service will be terminated immediately upon the publication of discharge orders.

5) Email accounts are assigned to individual personnel for their exclusive use. Users are responsible for all activities conducted with accounts assigned to them. Shared email accounts for specialized purposes, and with limited access to data, may be authorized by the Administrator. These accounts however are not be exempted from password standards and access control requirements.

6) The issuance of PCG e-mail accounts shall be limited to one (1) for each office/unit, and individual personnel. Moreover, as a bandwidth control measure, The PCG e-mail accounts for individual personnel shall only by used to those occupying key positions requiring access to such facility. All offices/units of the PCG are advised to forward their request for new District, station/office/units, sub-station/office/units and individual email accounts to

the Coast Guard Weapons Communications Electronics and Information Systems Command (CGWCEISC). **(Annex B – PCG E-mail Account Application Form)**

7) For uniformity and easy identification, the following email address format is established: <first name><dot><surname><serial number>@coastguard.gov.ph. For example: LT JUAN B DELACRUZ 0-22006 PCG will have an email address of juan.delacruz220062coastguard.gov.ph

   7.1 If the personnel have two or more first names, only the first will be indicated. Ranks and the word "junior' or abbreviations thereof will not be appended.

   7.2 For the Civilian employees, middle initials will be appended immediately after the first name to resolve similar first name, i.e., <first name><dot><middle initial><dot><Surname>@coastguard.gov.ph. For example JUAN B DELA CRUZ will have an email address of juan.b.delacruz@coastguard.gov.ph.

8) Passwords are to be kept secret. All users are responsible in maintaining the secrecy of the passwords for the accounts assigned to them. To maintain password integrity, the following standards must be followed:

   8.1 Passwords for accounts assigned to individuals may not be shared.

   8.2 A password must be changed if it is suspected or known that someone else knows the password.

   8.3 If the user has knowledge that another person knows or using their password, it is their responsibility to immediately report it to CGWCEISC.

   8.4 CGWCEISC may specify mandatory password standards that may include, but may not be limited to, length, content, and case restrictions, as well as requirements for periodic password change.

   8.5 Users are fully liable for all the activities conducted using the accounts assigned to them. Utmost care must be observed by all users to maintain secrecy and integrity of the passwords of their respective PCG email accounts **(Annex A – Guidelines on password Security)**

9) IT Staff and other authorized individuals may, by nature of assigned duties and in support of authorized activities, be exempt from any or all of these provisions regarding email accounts. Exceptions shall be authorized by the Deputy Chief of Coast Guard Staff for Maritime Communications, Weapons, Electronics & Information System, CG-11.

b. Conduct and Usage

1.) Users are responsible for data accessed, transmitted, copied, deleted, etc. done using their email account.

2.) Specific prohibitions relating to the reaction, transmission or storage of PCG email message are listed below:

2.1 Discrimination or harassment on the basis of age, race, color, gender, creed, marital status, national origin, disability, or sexual orientation.

2.2 An expression regarding personal political or religious beliefs;

2.3 An expression of rumour or gossip about any individual or group of individuals.

2.4 Any language and subject matter that is objectionable, offensive, obscene, threatening, or otherwise inappropriate;

2.5 Any communication to solicit for or promote commercials ventures, religious or political causes, outside the PCG or other non-job related solicitations;

2.6 Confidential and sensitive message, whether classified as such or deemed to be one;

2.7 Copyrighted materials; and

2.8 Any information that violates copyright laws.

3.) A user forwarding a message, which originate from someone else, may not make changes to that message without clearly disclosing the exact nature of the changes and the identity of the person who made the changes.

4.) If an electronic mail message is sent to a user by mistake, the user should stop reading as soon as they realize the message was not meant for them and notify the sender or System Administrator immediately.

5.) Usher shall establish distribution list on their contacts for multiple users to which they communicate regularly. The PCG" e-mail system is not intended to be used for general used for general mass to all PCG personnel.

c. Security

1) Users are responsible for the security of their electronic mail account password and any electronic mail that is vent a user account. To protect a

user account against unauthorized use, the following precautions should be taken:

1.1 Log off from, or lock access to the computer before leaving it unattended. If user id logon is left open, and someone else uses it, it will appear as if user sent the message and user will be held accountable

1.2 Do not give out passwords. Comply with the provision listed in para VI.a.7

2.) Data will not be copied and transmitted without the same access restrictions as those placed on the original data. This provision is not intended to restrict distribution of data resulting from public disclosure requests or the authorized release of information by the PCG.

3.) Unencrypted confidential and sensitive material must not be sent via electronic mail. Electronic mail messages may be intercepted, viewed, and used for non-approved purposes, especially when corresponding via the internet, a medium over which the PCG has no control.

4.) CGWCEISC shall not, as a matter of routine, inspect, monitor, or disclose electronic mail without the account holder's consent. Prior consent must be obtained in writing from the personnel when inspection, monitoring and disclosure have to be made. Nonetheless, subject to the requirements for authorization notification and other conditions specified in this policy, the policy, the PCG may deny the access to its electronic mail services and may inspect, monitor, or disclose electronic mail when.

4.1 Required by and consistent with law;

4.2 There is substantiated reason to believe that violations of law or of PCG policies have taken place.

4,3 When there are compelling circumstances; or

4.4 Under time-dependent, Critical operational circumstances.

5.) When the contents of email must be inspected, monitored, or disclosed without the holders consent, the following shall apply.

a. Authorization. Except in emergency circumstances, such actions must be authorized in advance and in writing by the Commandant, PCG. The advice of the Coast Guard Legal Service shall be sought prior to

b. Emergency Circumstances. In what emergency circumstances, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures describe in Section VI.c.5, above. If the action taken is

not subsequently authorized, the responsible authority shall seek to have the situation restored as closely as possible to that which existed before action was taken.

c. Notification. In either case, the responsible authority or designee shall, at the earliest possible opportunity that is lawful and consistent with other policies, notify the affected personnel of the action(s) taken and the reasons for the action(s) taken.

d. Alleged policy violations or inappropriate of PCG email systems shall be reported to the C,CGWCEISC to coordinate an investigation or to recommend an appropriate course of action. If an investigation is necessary, Commanding Officer of the alleged violator shall be responsible for conducting the investigation.

VII. RESPONSIBILITIES:

a.) Coast Guard Weapons Communications Electronics and Information System Command (CGWCEISC)

1. Provide policies and guidance to ensure that all personnel have email accounts.
2. Establish a system to ensure that the register of accounts is updated.

b.) Deputy Chief of Coast Guard Staff for Maritime Communications, Weapons, Electronics and Information System (CG-11).

1. Formulate information management and information technology doctrine for the PCG in support of the furtherance of internal communications functions.

2. Provide policies and guidance on the regulation and management of email accounts.

3. Provide oversight on the technical and equipment requirements of PCG electronic mail.

c.) Coast Guard Legal Service

Provide legal assistance and advice in matters concerning the inspection, monitoring and disclosure of mail accounts.

d.) Coast Guard Information System (CGIS)

1. Responsible for the administration of the mail server environment and Security System considerations

2. Provide the necessary equipment, training and services to adequately support the email requirements of the PCG.

3. Ensure usability of site, operational integrity and security of the computer and network supporting the email.

4. Implement training and curriculum requirements for the email administration personnel.

e.) System Administrator

1. Maintain, update the register of accounts;

2. Oversee the PCG's web mail and ensure compliance with current directives. Oversight includes monitoring as often as possible to ensure efficient delivery of mail services.

3. Reads and acts on user feedback and complaints about mail service functionality.

4. Serve as principal point of contact on all matters pertaining to administration of electronic mail.

VIII. EFFECTIVITY:

This SOP shall take effect upon publication.

BY THE COMMAND OF ADMIRAL HERMOGINO:

OFFICIAL:

LIEZEL B BAUTISTA
CDR PCG
Coast Guard Adjutant
05/03/19

EDUARDO D FABRICANTE
COMMO PCG
Chief of Coast Guard Staff