

Republic of the Philippines NATIONAL POLICE COMMISSION NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE OFFICE OF THE CHIEF, PNP

Camp BGen Rafael T Crame Quezon City

OCT 0 8 2020.

PNP MEMORANDUM CIRCULAR

NO.: 2020 -068

GUIDELINES AND PROCEDURES ON THE CREATION AND MANAGEMENT OF THE PNP E-MAIL SYSTEM

1. REFERENCES:

- a. Republic Act (RA) No. 10175 of September 12, 2012, also known as Cybercrime Prevention Act of 2012, "An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes";
- b. RA No. 10173 of August 15, 2012 also known as Data Privacy Act of 2012, entitled "An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes";
- c. RA No. 8792 of June 14, 2010 known as The Philippine E-Commerce Law, "An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions, Penalties for Unlawful Use Thereof and Other Purposes;
- d. National Computer Center Memorandum Circular 2003-01 entitled "Guidelines on Compliance to e-Commerce Act (RA No. 8792) and Stage 2 and 3 of the UN-ASPA Five Stages of e-Government;

 Administrative Order No. 39 entitled "Mandating Government Agencies to Migrate to the Government Web Hosting Service (GWHS) of the Department of Science and Technology-Information and Communications Technology Office (DOST-ICTO) dated July 12, 2013";
- e. Letter of Instruction 40/2012 (PNP e-mail System) dated October 8, 2012;
- f. Letter of Instruction 39/2012 (Management of Free Web-based E-mail Accounts) dated September 17, 2012;
- g. PNP Memorandum Circular (MC) No. 2012-003 dated May 20, 2012, entitled "Policy Guidelines on Security Consciousness and Secrecy Discipline in the Recording, Uploading, Posting or Dissemination of Information via the Internet or through other Information and Communications Technology (ICT) Devices by the PNP Personnel";
- h. PNP Memorandum Circular (MC) No. 2012-010 entitled "Guidelines on the Creation, Use and Maintenance of Websites at All Levels of the PNP Organization" dated March 25, 2011;
- C, PNP Letter of Instruction 03/09 (Spider-Web) dated November 11, 2009; and
- j. Approved PNP ICT Master Plan (S.M.A.R.T. Policing) dated November 16, 2018.

ERTIFIED TRUE COPT

AICHAELS MACAPAGAL

Police Major administrative Officer

Page 1 of 13

2. RATIONALE:

This Memorandum Circular (MC) will ensure the creation and management of the PNP e-mail accounts of all PNP offices/units and its personnel for official communication purposes through maximized utilization of the existing technology in support to the initiatives of the PNP ICT Master Plan.

3. SITUATION:

In today's environment, e-mail or electronic mail is considered as one of the vital tools for most organizations as it can deliver significant business benefits when used appropriately. As a method of communication, it is quick, affordable, convenient, and entails less paper in transmitting communications. However, carelessness or negligence in using e-mail, particularly the free web-based e-mail services may result to potential problems such as leakage of sensitive information, propagation of viruses and other malicious software that would destroy the data, network and other ICT resources of the organization, and in extreme cases, may lead to complaints or legal issues against the PNP office/unit or its personnel.

In response to this, all Philippine government agencies are required to use the domain.gov.ph in its URL (Uniform Resource Locator), and have it registered at Government Online Services Division under the Department of Information and Communications Technology (formerly DOST-ASTI) pursuant to AO 39. The agency shall be assigned with a primary domain. In the case of the PNP, the pnp.gov.ph and its subordinate offices/units will become part of the primary domain called subdomain for offices/units e-mail. The PNP website as primary domain is being hosted, administered, and managed by the Department of Information and Communications Technology (formerly DOST-ICTO) while websites of subordinate PNP offices and units pursuant to LOI 03/09 (Spider Web) are subscribed to private hosting provider and registered as subdomain to carry the pnp.gov.ph in its domain name (e.g. dc.pnp.gov.ph).

Official e-mail accounts carrying the PNP domain (e.g. tcds@pnp.gov.ph) are likewise hosted and managed by the DICT but limited to PNP offices/units/stations and personnel holding key positions. However, request for additional individual e-mail accounts are subject to endorsement of ITMS to DICT for approval on first come, first serve basis. PNP personnel other than those holding key positions tend to use free web-based e-mail accounts in work-related communications. Oftentimes, free webbased e-mail accounts such as Yahoo, Gmail or Hotmail that are being used by PNP personnel in official transactions (e.g. foreign training, inter-agency engagements or subscriptions intended for the office) are not accepted as official e-mail address.

The use of free web-based account is disadvantageous to the organization since personal e-mail accounts cannot be turned over nor allowed access by another in case of relief, retirement or termination of personnel leaving classified documents/information in the hands of unauthorized person. Access for valuable documents or historical information transmitted through personal e-mail account then becomes a challenge for retrieval of the concerned office since it is discretionary to the owner. Moreover, the organization as well as the user of free e-mails have no control in changing the privacy policy of free e-mail providers, and the extent of privacy

CERTIFIED TRUE COPY

MICHAETS MOCAPAGAL

Page 2 of 13

intrusion is unknown considering that "free" e-mail host can use information to generate revenue.

Recognizing the need for legitimacy in official transactions engaged by individual PNP personnel for inbound and outbound communication and giving emphasis to security of electronic documents as mandated by the Data Privacy Act of 2012, it is necessary that the PNP personnel must have official e-mail accounts provided for and managed by the PNP.

4. PURPOSE:

This MC provides guidelines and procedures in the creation of PNP individual email and management of PNP E-mail System including the DICT issued emails.

5. DEFINITION OF TERMS:

- a. Database (DB) is an organized group or set of inter-related information about a subject that can be processed, retrieved, analyzed, and used drawing conclusions and making-decisions.
- b. DICT Hosted E-mail Service is a system established by the PNP under LOI 40/2012; developed and maintained by Information Technology Management Service under the sub-domain pnp.gov.ph that provides a web-based e-mail to be used by the PNP from the National Headquarters down to the Police Stations.
- c. E-mail refers to the digital mechanism for exchanging messages through Internet or Intranet communication platforms.
- d. E-mail System is the network of computers handling electronic mail on the Internet. This system includes user machines running program that compose, send, retrieve, and view messages, and agent machines that are part of the mail handling system.
- e. Free Web-based e-mail are free web-based e-mail systems hosted by foreign entities like Yahoo Mail, Gmail, Hotmail, and others.
- f. Hardware is the electronic and physical components, boards, peripherals and equipment that make up a computer system as distinguished from the programs (software) that tell these components what to do. It is the physical components consisting of the input devices, central processor, output devices, and storage devices.
- g. Information and Communications Technology (ICT) is the totality of the electronic means employed to systematically collect, process, store, present, and share information to end-users in support of their activities. It consists of computer systems, office systems, consumer electronics, and telecommunications technologies, as well as networked information infrastructure the components of which include the telephone system, the Internet, fax machines, computers and its accompanying methodologies, processes, rules, and conventions. A combination of computer technology, microelectronics applications and

erom the deignal

MICHAELS MACAPAGAL

Page 3 of 13

communications information techniques and methods, it encompasses the use of computers, data communications, office systems technologies, as well as any technology that deals with modern day application of computing and/or communication. It can also be seen as the marriage of information technology and data communication.

- h. Information System is a system of major processes or operations which facilitates the storage, processing, retrieval, and generation of information for decision-making, planning, controlling and monitoring purposes. It also refers to a group of related processes (manual or computerized) designed to generate information for the exclusive support of a major functional area of an organization.
- Information System Owner is the PNP office/unit that legally owns the Information System.
- j. Internet is a worldwide interconnection of millions of computer networks and databases. It is popularly referred to as the Information Superhighway, the Web, or simply as the Net.
- k. Internet Service Provider (ISP) is an entity or company that provides connection services to the Internet. Access to the Internet is provided through its facility linked to the Internet. Such service provider may be a commercial entity, an institution, a university, or any other entity that has already a link to the Internet.
- Local Area Network (LAN) is a network of computers that are in the same general physical location, usually within a building or a campus communications network that serves users within a confined geographical area.
- m. Server is a computer that shares its resources, such as printers and files, with other computers on the network. One example of this is a Novell network Server which shares its disk space with a workstation that does not have a disk drive of its own. A computer that makes services, as access to data files, programs, and peripheral services, available to workstations on a network.
- n. Software is a set of instructions encoded to a computer (and its peripheral equipment) to execute a command or to process data. It uses a computer-understandable language. These are the non-physical components, which may be an operating system, a development language, database management system, network management software, set of computer tools and utilities, or an applicable package, as well as the machine-coded instructions that direct and control the different hardware facilities.
- Secured Socket Layer (SSL) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

CROM THE ORIGINALP. User/Client – is the user of a workstation connected to a network.

CERTIFIED TRUE COPY

CROM THE ORIGINALP.

MICHAEL S WACAPAGAL

Page 4 of 13

- q. Virtual Private Server (VPS) refers to that which the user perceives as a dedicated/private server even though it is installed on a physical computer running multiple operating systems.
- r. Web Hosting Service is the type of internet service that includes website accessibility, data storage, and email service that can be accessed through the World Wide Web (www).
- s. Workstation is a networked personal computing device that accepts, processes, stores, and outputs data at high speeds according to programmed instructions.

6. GUIDELINES:

- a. General Guidelines:
 - Professional Tone PNP officials and personnel should use the same level of care and draftsmanship in e-mail transmission as they do with respect to official memo/correspondence. Attached memo/correspondence sent through e-mail should be professionally written with a professional tone, official form and style should be used adopting the format prescribed under PNP Memorandum Circular No. 2019-013 dated March 5, 2019;
 - 2) Prohibited E-mail Content and Usage All PNP personnel are prohibited to transmit any e-mail over the PNP systems that contain illegal, defamatory, insulting, vulgar, rude, disruptive, offensive, derogatory, harmful, or immoral content. Prohibited transmission include, but are not limited to sexually-explicit or sexually oriented materials, cartoons or illustrations, jokes, romantic oriented materials, anything that could be deemed to be sexually harassing, sexual innuendos or references, propositions of love, whether wanted or unwanted, ethnic or racially oriented references or slurs, or any other materials that could be considered by the recipient to constitute sexual harassment or harassment based on sex, sexual orientation, race, ethnicity, national origin, religious or political beliefs or practices, and/or for entertainment or gaming purposes;
 - 3) Official Use The PNP official email accounts shall be used for official and work-related purposes and not in violation of the above prohibitions. Utilization of free web-based e-mail service (Gmail, Hotmail, Yahoo Mail, etc.) in the official PNP electronic communications shall be unauthorized. It will also be used in other official transactions such as but not limited to sending of copies of personnel orders such as assignment and reassignment orders, promotion orders, designation orders and the like; sending results of administrative transactions such as Training Order of Merit, Annual Physical Examination, Laboratory Results, Neuro Psychiatric Examination, Personnel Evaluation Report, and the like which shall be a digital copy of the PNP Personnel;



- 4) Ownership All information and messages that are created, sent, received, or stored in the E-mail System of the PNP is the sole property of the PNP. Individual e-mail accounts shall only be used by the PNP personnel for official purposes and work-related communication;
- 5) E-mail Review All e-mails are subject to the right of the PNP to monitor, access, read, disclose, and use without prior notice to the originators and recipients of such e-mail. E-mail may be read by the Assistant Supervisor for the PNP for any violations of law, breaches of the PNP policies, communications harmful to the organization, or for any other reasons relative to work and the PNP as a whole;
- Security The PNP E-mail System users shall not disclose or share their credentials, and must exercise security and accountability in the use of e-mail accounts;
- Presumption of Privacy/Confidentiality E-mail communications sent through the PNP E-mail System shall be highly confidential except for purposes of investigation and disciplinary action;
- 8) Message Retention and Creation PNP personnel should be careful in creating e-mails. Even when a message has been deleted, it may still exist in printed version, be recreated from a back-up system, or may have been forwarded to someone else. Please note that appropriate electronic messages may be saved if necessary;
- Viruses Any files downloaded from e-mail received from outside PNP sources must be scanned with the virus detection software of the PNP; and
- 10) Back up Facility Due to resource limitation, back up of PNP personnel e-mail accounts shall be the sole responsibility of the owner, while the official office/unit email accounts shall be maintained by ITMS through its backup facility for the purpose of redundancy to ensure business continuity.

b. Specific Guidelines:

All Admin Officers of offices/units shall be the designated E-mail Account Administrator with the following functions:

- 1) Maintain and update status of official e-mail accounts to ITMS;
- 2) Ensure the systems security for the e-mail service;
- Update the operating system and application software of the computers and other patches as necessary;
- Responsible for providing technical assistance to the PNP offices/units using the PNP official e-mail;

FROM THE ORIGINAL

MICHAELS MACAPAGAL

- 5) Act as focal person during cascading and user's training of the e-mail system;
- Monitor compliance and use of office/unit and personnel official PNP e-mail account; and
- 7) Perform other tasks as directed.

c. Responsibilities

1) TCDS

- a) Designated as Overall Supervisor in the implementation of this MC; and
- b) Perform other tasks as directed.

2) TDPRM

- a) Designated as Overall Assistant Supervisor for Personnel E-mail Accounts and in-charge in the implementation of the E-mail System for Personnel E-mail Accounts;
- b) Act as the Policy Administrator for Personnel E-mail Accounts;
- c) Issue supplemental directives consistent with the purpose and intent of this MC to clarify, restore order, and set direction in the use and security of Personnel E-mail Accounts; and
- d) Perform other tasks as directed.

3) TDPL

- a) Designated as Overall Assistant Supervisor for Office/Unit E-mail Accounts and in-charge in the implementation of the E-mail System for Office/Unit E-mail Accounts;
- b) Act as the Policy Administrator for Office/Unit E-mail Accounts;
- c) Issue supplemental directives consistent with the purpose and intent of this MC to clarify, restore order, and set direction in the use and security of Office/Unit E-mail Accounts; and
- d) Perform other tasks as directed.

4) TDC

- a) Provide funds for the implementation of this MC; and
- b) Perform other tasks as directed.

FROM THE ORIGINAL WICHAEL SMACAPAGAL

Page 7 of 13

5) TDL

- a) Provide logistical requirements for the implementation of this MC;
 and
- b) Perform other tasks as directed.

6) TDICTM

- a) Assist in the implementation and monitoring of this MC and the Email System;
- Review and update this MC to ensure that the guidelines are appropriate and relevant to the existing organizational needs and operational conditions;
- Research on security issues and development of e-mail services and applications to suit the needs of the PNP; and
- d) Perform other tasks as directed.

7) D, ITMS

- a) Designated PNP E-mail Super Administrator or Overall Administrator;
- b) Submit IMPLAN for the implementation of this project;
- Provide central backup facility and responsible for the day-to-day maintenance operations of the PNP E-mail System nationwide;
- d) Ensure system security for the e-mail service through renewal of Secured Socket Layer (SSL) certificate and regular checking and review of audit trails;
- e) Update the necessary operating system and application software and other patches of the PNP Email System servers:
- Responsible for providing technical assistance to the PNP offices/units using the PNP official e-mail;
- g) Provide basic user training on the user interface of the said e-mail system for both operators and executives;
- h) Designate ITPOs as focal persons in the different PNP offices/units responsible for cascading, implementation, maintenance, and user's training; and
- i) Perform other tasks as directed.

8) Other D-Staff, PROs, NSUs and P-Staff

 Responsible for the implementation of this project in their respective offices/units;

CERTIFIED TRUE COPY FROM THE ORIGINAL

MICHAELS MACAPAGAL

- b) Responsible for the proper use of the email accounts in their respective offices/units and personnel;
- c) Ensure internet connectivity; and
- d) Perform other tasks as directed.

d. Coordinating Instructions:

- 1) All PNP Information Systems Owners shall utilize the usage of the PNP E-mail System in their Information Systems such as the PNP Daily Online Personnel Accounting (PDOPA); Personnel Accounting Information System of DPRM in sending Personnel Transaction Orders such as but not limited to personnel orders such as assignment and reassignment orders, promotion orders, designation orders, and the like; and
- 2) All PNP offices/units shall include the utilization of the PNP E-mail System in the development of information systems such as Information Systems for PNP Health Service for Laboratory, Annual Physical Examination; Directorate for Human Resources Doctrine Development for Training Orders, Order of Merit, and the like.

7. PROCEDURES:

The following procedures on the creation and arrangement of PNP e-mail system shall be observed:

a. Creation of E-mail Account

1) Personal Email Accounts (for all PNP Personnel)

All PNP personnel shall have official e-mail accounts. Request for creation of additional official e-mail accounts for personnel shall be submitted to TDPRM for approval before creation by ITMS.

2) Office and Unit Email Accounts

All PNP offices/units shall be assigned, and use an official e-mail account. All offices/units shall have an e-mail account per division with at least two (2) designated users or operators who shall be responsible for its usage and maintenance. Request for the creation of additional e-mail accounts intended for sections of a PNP office/unit shall be submitted to TDPL for approval before creation by ITMS.

a) Naming Convention

For uniformity and easy recall, the corresponding naming convention for PNP offices/units and personnel e-mail address shall be created as shown below:

(1) Command Group and its offices

Format: cmdgrp@pnp.gov.ph Sample: tcds@pnp.gov.ph

FROM THE ORIGINAL

MICHAEL S MACAPAGAL

Format for Offices:

Format: office/division.cmdgrp@pnp.gov.ph

Sample: admo.tcds@pnp.gov.ph

(2) D-Staff and its offices

Format: directorate@pnp.gov.ph Sample: dictm@pnp.gov ph

Format for Offices:

Format: office/division.directorate@pnp.gov.ph

Sample: ppd.dictm@pnp.gov.ph

(3) NOSU/NASU and its offices

Format: NOSU/NASU@pnp.gov.ph

Sample: itms@pnp.gov.ph

Format for offices:

Format: offices/division.NOSU/NASU@pnp.gov.ph

Sample: issd.itms@pnp.gov.ph

(4) P-Staff and its offices

Format: p-staff@pnp.gov.ph Sample: ias@pnp.gov.ph

Format for Offices:

Format: office/division.pstaff@pnp.gov.ph

Sample: admin.ias@pnp.gov.ph

(5) PROs, NCRPO and its offices

Format: cmdgroup.regionaloffice@pnp.gov.ph

Sample1: ord.pro1@pnp.gov.ph Sample2: odrda.procor@pnp.gov.ph Sample3: odrdo.pro4b@pnp.gov.ph Sample4: ocrs.ncrpo@pnp.gov.ph

Format for offices:

Format: office/division.regionaloffice@pnp.gov.ph

Sample: romd.ncrpo@pnp.gov.ph

R1 - rprmd.ncrpo@pnp.gov.ph

R2 - rid.ncrpo@pnp.gov.ph

R3 - romd.ncrpo@pnp.gov.ph

R4 - rlrdd.ncrpo@pnp.gov.ph

R5 - rcadd.ncrpo@pnp.gov.ph

R6 - rcd.ncrpo@pnp.gov.ph

R7 - ridmd.ncrpo@pnp.gov.ph

R8 - rlddd.ncrpo@pnp.gov.ph

R9 - rpsmd.ncrpo@pnp.gov.ph

R10- rictmd.ncrpo@pnp.gov.ph

FROM THE ORIGINAL

MICHAEL SMACAPAGAL

Police Major

(6) Districts and its Major Cities and offices

Format: district.regionaloffice@pnp.gov.ph

Sample: spd.ncrpo@pnp.gov.ph

Format District cities:

Format: city.district.regionaloffice@pnp.gov.ph

Sample: makati.spd.ncrpo@pnp.gov.ph

Format District Offices:

Format: office/division.district.regionaloffice@pnp.gov.ph

Sample: did.spd.ncrpo@pnp.gov.ph

(7) Format District City Stations:

Format: stn.city.district.regionaloffice.@pnp.gov.ph

Sample: stn1.makati.spd.ncrpo@pnp.gov.ph

(8) RMFBs and its Offices/Cities

Format: rmfb.regionaloffice@pnp.gov.ph

Sample: rmfb.pro2@pnp.gov.ph

(9) RMFBs and its Offices/Cities

Format: rmfb.regionaloffice@pnp.gov.ph

Sample: rmfb.pro2@pnp.gov.ph

(10) Provincial Police Office/City Police Office/Station

Format: ppo/cpo.regionaloffice@pnp.gov.ph

Sample: cagayanppo.pro2@pnp.gov.ph

Sample: tuguegaraocpo.pro2@pnp.gov.ph

(11) Municipal Police Station/Police Community Precinct

Format: mps.ppo.regionaloffice@pnp.gov.ph

Sample1: sta_ana.cagayanppo.pro2@pnp.gov.ph

Sample2: aparri.cagayanppo.pro2@pnp.gov.ph

(12) Official Personal Account:

Sample: firstname.lastname@pnp.gov.ph

juan.delacruzjr@pnp.gov.ph

for duplicate (add numeric sequence): firstname.lastname01@pnp.gov.ph

juan.delacruzjr01@pnp.gov.ph

juan.delacruzjr02@pnp.gov.ph

b. Usage (general description)

The designated user or operator of the office/unit and personnel e-mail account shall adhere to the following rules:

- 1) Immediately delete the message when it contains spam, chain letter, pornographic material, or other non-business-related information;
- SERTIFIED TRUE COPY 2) Shall not use the e-mail to propagate a virus or other malicious software:

Page 11 of 13

- 3) Use a virus scanner or other tools, as recommended by ITMS, to clean a document or file suspected to contain a virus or other malicious software:
- 4) Take appropriate action to protect downloaded messages, documents or files that contain sensitive information; and
- 5) Shall not disclose any information contained in the e-mail communication except to his immediate superior or other concerned authorities of the office.

c. Turn-over of Office/Unit E-mail account

PNP personnel who will be designated as e-mail user or operator of the concerned office/unit and is applying for transfer or retirement from the service shall be required to turn over the e-mail account details to the Admin Officer or Chief of Office.

The e-mail account details shall contain the following information:

- 1) Complete e-mail address;
- 2) Complete name and designation, active contact number/cellphone number and the office/section that uses the e-mail account to be turned over: and
- Passwords.

E-mail system administrator shall update the e-mail contacts of their respective Command Group, Heads of Offices/Units, and personnel.

d. Deletion of Personnel E-mail Accounts

An e-mail account that needs to be deactivated shall be endorsed in writing by the respective Admin Officer to TDPRM for official personnel accounts and TDPL for office accounts. Prior to the deletion, all official communications in the mailboxes that have historical value shall be backed up by the email system super administrator of the Information System Strategic Division (ISSD), ITMS. Destruction of any information, whether printed or not, should be in accordance with the guidelines and procedures set by the Directorate for Intelligence (DI).

After an e-mail account is deleted, the account owner or authorized user shall immediately advise other PNP offices/units or personnel of the fact together with the replacement account, in case another one was created.

Circumstances when e-mail account shall be deactivated are as follows:

- 1) Death, retirement, resignation, dismissal from the service; and
- Dissolution of an Office or Unit or any office, division, or section under it.

TERTIFIED TRUE COPI FROM THE GRIPPINAL MICHAELSMACAPAGAL

Police Major

8. ADMINISTRATIVE SANCTIONS:

Any violation(s) of the provisions of this MC shall be dealt with administratively pursuant to NAPOLCOM Memorandum Circular No. 2016-002 and other applicable laws, rules, and regulations.

9. REPEALING CLAUSE:

All existing PNP directives and other issuances which are contrary to and/ or inconsistent with the provisions of this MC are hereby rescinded or modified accordingly.

10. EFFECTIVITY:

This MC shall take effect after 15 days from filing a copy thereof at the UP Law Center in consonance with Section 3, Chapter 2, and Book VII of Executive Order 292 otherwise known as the "Revised Administrative Code of 1987," as amended.

CAMILO PANCRATIUS P CASCOLAN

Police General Chief, PNP

Distribution:

Command Group

D-Staff

P-Staff

D, NSUs

RD. PROs

Copy Furnished: SPA to SILG CPNP Ln: 20 S083171
S083171
OCT () 8 2020

CERTIFIED TRUE COPY
FROM THE ORIGINAL

MICHAELS MACAPAGAL

Police Major