



Republic of the Philippines
NATIONAL POLICE COMMISSION
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
OFFICE OF THE CHIEF, PNP
Camp BGen Rafael T Crame, Quezon City

JAN 13 2021

MEMORANDUM CIRCULAR
NO.: 2021-004

**STANDARD PNP OFFICE/UNIT IDENTIFICATION CARD AND PNP SAFETY
ACCESS MANAGEMENT SYSTEM (PNP SAMS)**

1. REFERENCES:

- a. Republic Act (RA) No. 11032, otherwise known as the "Ease of Doing Business and Efficient Government Service Delivery Act of 2018," and its Implementing Rules and Regulations (IRR);
- b. RA No. 9485, otherwise known as the "Anti-Red Tape Act of 2007";
- c. National Computer Center Memorandum Circular (MC) 2003-01 "Guidelines on Compliance to E-Commerce Act (RA 8792) and Stage 2 and 3 of the UN-ASPA Five Stages of E-Government";
- d. PNP MC No. 2012-003 "Guidelines on Security Consciousness and Secrecy Discipline in the Recording, Uploading, Posting or Dissemination of Information and Communications Technology (ICT) Devices by PNP Personnel";
- e. Policy on the Operation of the Systematic Data Scheduler (SDS) dated May 10, 2019;
- f. PNP E-mail System (PES) dated October 8, 2020; and
- g. LOI KALASAG 2008.

2. RATIONALE:

This Memorandum Circular (MC) provides the guidelines and procedures on the Creation, Usage, and Disposal of Standard PNP Offices Identification Card, and creation of the PNP Visitor Entry and Systematic Tracking as part of the PNP's COVID-19 prevention and mitigation strategy to monitor and trace the movement of PNP personnel nationwide.

3. SITUATION:

In the PNP's shift to new normal activities due to the pandemic, it is no surprise that it shifted a lot of activities to digital space where anything is just a punch of a keyboard or a click of the mouse.

At present, the PNP COVID-19 Data (CODA) Project, one of the PNP's COVID-19 response and mitigation initiatives, is making a lot of progress in terms of Geo-tagging, and Camp QR Code Entry and Visitor Registration and Movement capabilities.


CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

Also, the Standard PNP Office Identification Card or the Safety Access Management System (SAMS) which was designed to complement the PNP CODA Entry and Visitor Tracking Module has been implemented at the Office of the Chief, PNP and ready for full implementation down to the police station level.

However, electronic form of sensitive information travelling online public via telecommunication infrastructure due to the PNP's new normal is vulnerable to snooping, hijacking, and other malicious activities by anyone who has discord against the PNP or the State. Information stored in the server machines of e-mail hosting and/or cloud server providers could be accessed, legally or illegally, by anyone who maintains the servers.

At the advent of technological advancements in the PNP, the SAMS is formulated to provide updated and real-time tracing of PNP personnel entering PNP camps and offices to ensure safe movement, and ease of access as well as to keep abreast with the ever-changing world of information technology.

To address the issue of information security, it must be emphasized that communications sent via PNP SAMS must be secured and can only be accessed with proper credentials issued from the system administrator and/or respective PNP office/unit network administrators. PNP SAMS server shall be hosted by Information Technology Management Service (ITMS) as part of the PNP CODA.

4. PURPOSE:

This MC shall serve as the working plan in setting procedures for the design, printing, issuance, and disposal of the Office ID and the development, deployment, user's training, usage, and maintenance of the PNP SAMS; standardize the design of PNP Office Identification card; create a portal that aims to deliver an automated, online private, and "real-time" COVID-19 detection strategy throughout the country; ensure the proper creation, turn-over, update or deactivation of accounts created in the PNP SAMS; ensure the proper creation, and/or disposal of expired PNP Office Identification Card; remind the users/operators periodically about data privacy and security; and designate tasks and responsibilities to certain office/unit and/or personnel of the PNP.

5. DEFINITION OF TERMS:

- a. Database (DB) – an organized group or set of inter-related information about a subject that can be processed, retrieved, analyzed, and used in drawing conclusions and making-decisions;
- b. PNP e-Mail Service (PES) – is a system established by the PNP under LOI 40/2012 which aims to provide a web-based electronic mail to be used by the PNP from the National Headquarters down to the police stations; developed and maintained by the Department of Information Communication Technology; PNP is under the sub-domain pnp.gov.ph;

AUTHENTICATED BY:


CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

- c. PNP One Network (PON) – is a system established by the PNP which aims to provide single internet service provider to all PNP offices/units;
- d. E-mail – the digital mechanism for exchanging messages through Internet or Intranet communication platforms;
- e. File Server – is a computer attached to a network that provides a location for shared disk access;
- f. Free Web-based e-Mail – are free web-based electronic mail systems hosted by foreign entities like Yahoo Mail, Gmail, Hotmail, and others;
- g. Hardware – 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;
- h. 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 component of which includes the telephone system, the Internet, fax machines, computers, and its accompanying methodologies, processes, rules, and conventions. A combination of computer technology, microelectronics applications, and 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;
- i. Information System – 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;
- j. Information System Owner – PNP office/unit that legally owns the Information System;
- k. Internet – 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;

AUTHENTICATED BY:


CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

- l. Internet Service Administration Team (ISAT) – a team created through CMC 14-13 dated April 2, 2012 with a task of ensuring proper use of the internet in PNP offices/units;
- m. Internet Service Provider – 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;
- n. Intranet – a private network accessible only to an organization's staff. Often, a wide range of information and services available on an organization's internal network;
- o. Local Area Network (LAN) – 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;
- p. Network Administrator – the person designated in an organization whose responsibility includes maintaining computer infrastructures with emphasis on networking;
- q. Network Layout – the logical or physical diagram of both the existing and proposed interconnection of computers and associated devices to provide end-users with a means of communicating and receiving information electronically without being limited by geographical distance;
- r. Quick Response Code (QR Code) – is a type of matrix barcode (or two-dimensional barcode) first designed in 1994 for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. In practice, QR codes often contain data for a locator, identifier, or tracker that points to a website or application. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to store data efficiently; extensions may also be used;
- s. PNP COVID-19 Data – the current information system providing data on the PNP COVID-19 status;
- t. Server – 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;
- u. Software – a set of instructions encoded to a computer (and its peripheral equipment) to execute a command or to process data. It

AUTHENTICATED BY:

CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

Page 4 of 13


CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

Page 5 of 13

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:

- v. Software License – agreement between a user and a software house, giving details of the right of the user to use or copy software; a legal right granted for a company/agency to run a software program. For every software program used, a license is needed and granted to the user (company or agency) and is documented in a license agreement;
- w. User/Client – the user of a workstation connected to a network;
- x. Virtual Private Network or VPN – is used to create a safe, encrypted connection over a less secure network, such as the public internet;
- y. Virtual Private Routed Network or VPRN – a Layer 3 VPN; and
- z. Workstation – a networked personal computing device that accepts, processes, stores, and outputs data at high speeds according to programmed instructions.

6. GUIDELINES:

a. General Guidelines:


- 1) As a general rule, all PNP offices/units Identification Card shall conform to the design specified by this MC to possess the requirements needed by the PNP SAMS;
- 2) Standard PNP Office Identification Card shall be exclusively and confidentially printed at the issuing office to avoid leaking the security features and design of the card;
- 3) PNP CODA shall be capable of reading the QR Code placed in the PNP Office ID Card or PNP SAMS upon scanning and at the same time return real-time data from the PNP CODA Server;
- 4) PNP SAMS shall be treated as an electronic logbook of the movement of personnel from office to another office;
- 5) PNP SAMS shall be the official visitors' electronic logbook in all PNP camps and offices;
- 6) PNP SAMS shall be a module of the PNP CODA and PAIS;
- 7) PNP SAMS shall be accessible via online and connected to the PNP CODA via application programming interface (API) or browser-based;


CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

- 8) All PNP One Network (PON) Focal Persons shall ensure inter-connectivity with the PNP SAMS;
- 9) PNP Email System (PES) shall be the official E-mail that will be used in the PNP SAMS;
- 10) All PNP SAMS Administrators must ensure that they are logged in to the PNP SAMS 24/7;
- 11) All PNP personnel moving from their place of work to another PNP building/place must scan their Office ID at the PNP SAMS Scanner;
- 12) The PNP CODA server shall serve as the central repository of all electronic data such as but not limited to movements of PNP personnel and civilians in and out the PNP camps through the implementation of the Camp QR Code Entry and Visitor Registration;
- 13) The PNP SAMS under the existing PNP CODA shall serve as the main personnel tracking/monitoring system of the PNP. All other similar/related systems currently existing should conform to and not hamper the effective day to day operations/implementation of the PNP SAMS;
- 14) All D-Staff/P-Staff/PROs/NSUs personnel shall have a viewer's access to the PNP SAMS upon request;
- 15) All D-Staff/P-Staff/PROs/NSUs Building Commanders/Heads of Office are automatically tasked as PNP SAMS Supervisor;
- 16) All Team Leaders of PNP checkpoints are automatically tasked as PNP SAMS Supervisor; and
- 17) The PNP CODA and PAIS database shall be the source of data of PNP SAMS and shall be updated and agile to be able to promptly adapt to the new needs of the PNP organization.

b. Specific Guidelines:

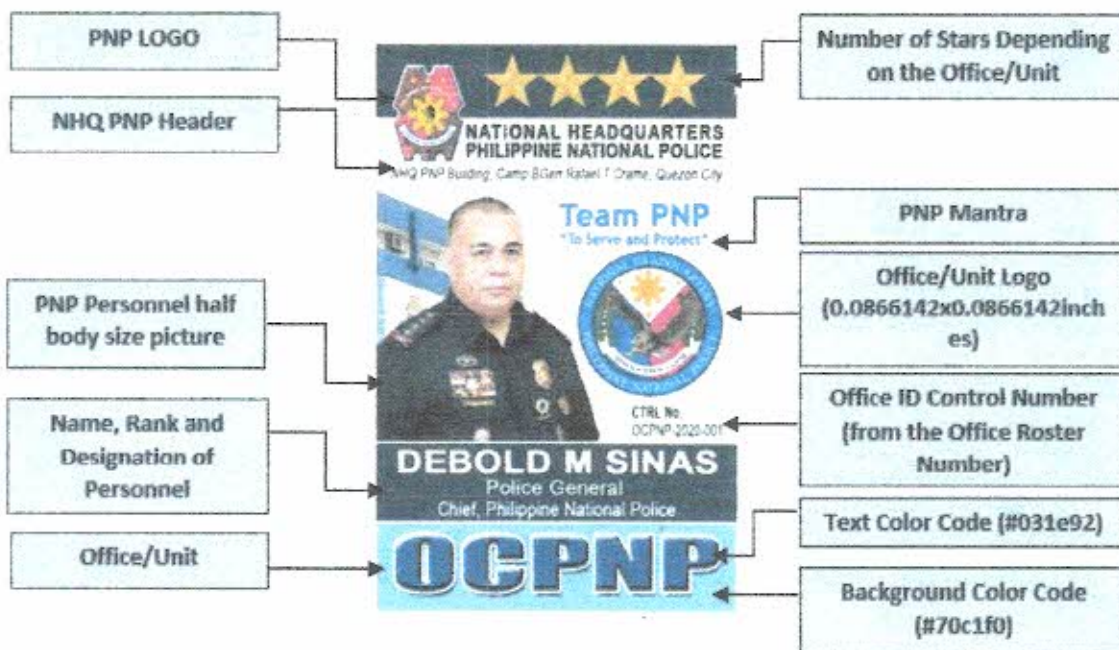
- 1) Individual QR code generated in the PNP CODA shall be utilized in the PNP Office Identification Card;
- 2) Only the official PES shall be used as change password credential in the PNP SAMS;
- 3) Outgoing duty of the PNP camp gates/offices must print, sign, and submit his/her Tour of Duty (TOD) Report through the PNP SAMS/PNP CODA report tab upon the end of his TOD;
- 4) PNP SAMS administrator shall be responsible for reviewing/auditing the logs of their respective PNP SAMS;

AUTHENTICATED BY:

CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

5) This PNP Office Identification Card Design shall be observed:

PNP Standard Office ID Card (Front)

Features



AUTHENTICATED BY:

Cherry May R. Padla
CHERRY MAY R PADLA
 Police Lieutenant Colonel
 Administrative Officer

Page 7 of 13



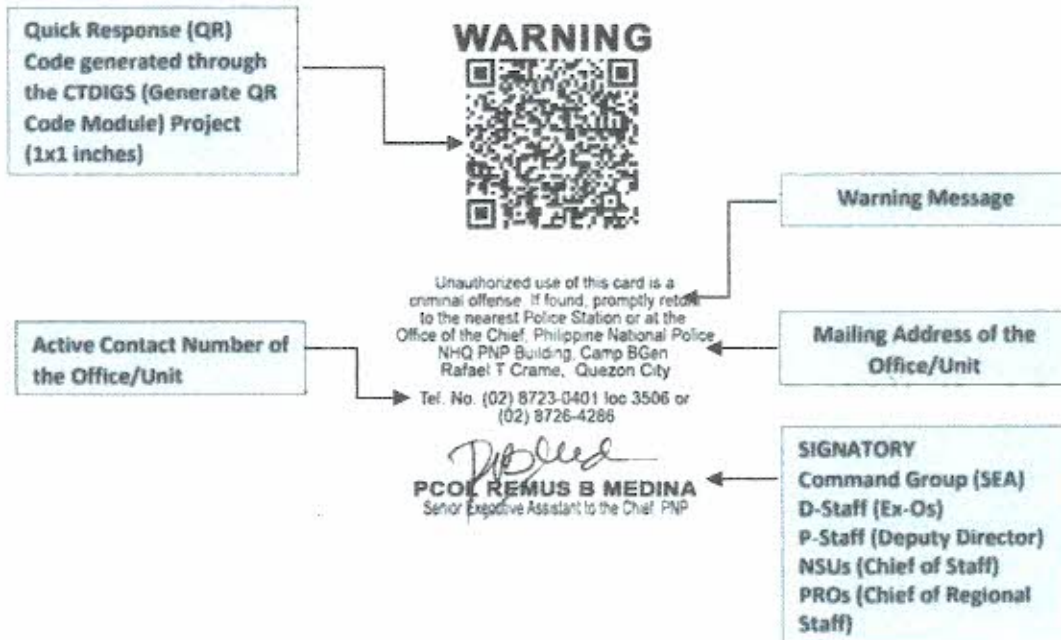
AUTHENTICATED BY:

Cherry May R. Padla
CHERRY MAY R PADLA
 Police Lieutenant Colonel
 Administrative Officer

Page 8 of 13

PNP Standard Office ID Card (Back)

Features



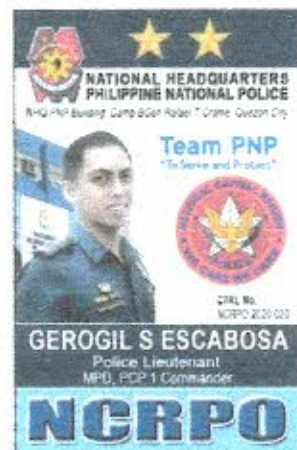
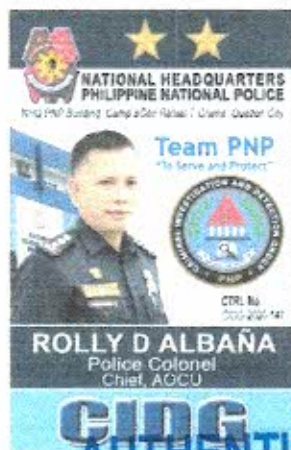
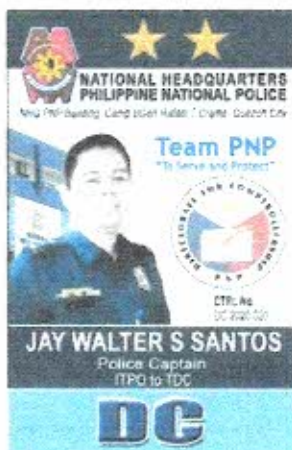
PNP Standard Office ID Card (Front)

D-Staff

NOSU

NASU

PRO

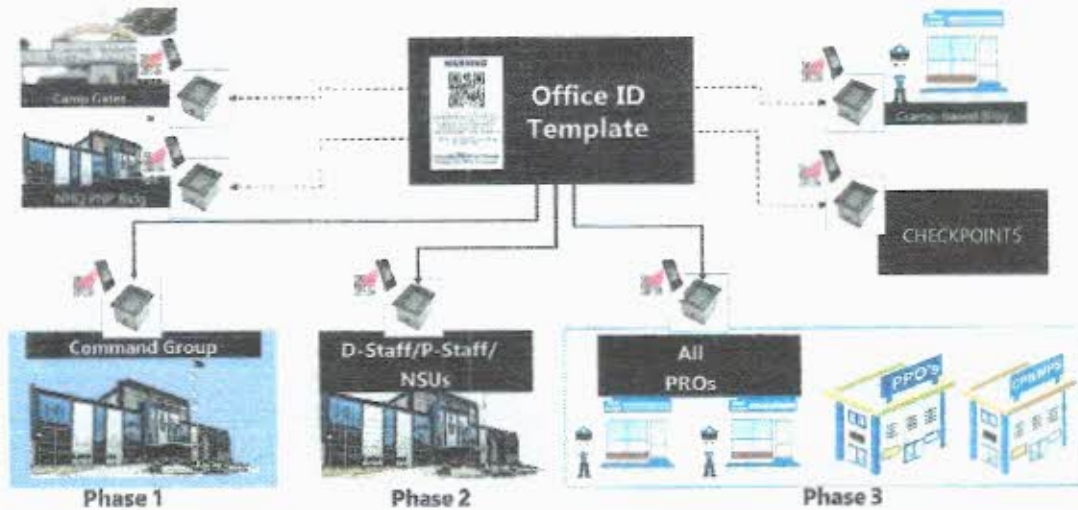


AUTHENTICATED BY:

Cherry May R Padla
CHERRY MAY R PADLA
 Police Lieutenant Colonel
 Administrative Officer

8) This Concept of Operation shall be observed in implementing the project:

CONCEPT OF OPERATIONS



c. Tasks:


1) TCDS

- a) Designated as Overall Supervisor in the implementation of this MC;
- b) Supervise all phases of the PNP Standard Office ID and PNP SAMS program from crafting of the Terms of Reference, development, deployment, training, utilization, maintenance, and improvements/innovations; and
- c) Oversee the implementation of the PNP Standard Office ID and PNP SAMS in the PNP.

2) DICTM;

- a) Assistant Overall Supervisor in the implementation of this MC;
- b) Assist the overall supervisor in the successful implementation of the PNP SAMS;
- c) Supervise PNP offices/units in the implementation of this MC;
- d) Fast track the utilization of the PNP e-Mail System and PNP One Network;
- e) Research on security issues of PNP SAMS, PNP E-mail System, and other applications to suit the needs of the PNP; and

AUTHENTICATED BY:
f) Perform other tasks as directed.


CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

3) **SDS**

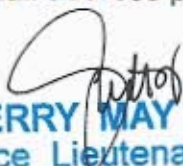
- a) Designated as co-OPR of this MC in coordination with the ITMS;
- b) Designate C, MISS, OTCDS to manage, administer, and supervise all phases of the PNP SAMS Project from development, utilization, maintenance, and improvements/innovations in coordination with the ITMS;
- c) Ensure that appropriate funds are allocated to support the operation and maintenance of the PNP SAMS Server, QR Code Scanners, ID Printers, etc in coordination with the Directorate for Comptrollership (DC);
- d) Task C, MISS, OTCDS to conduct quarterly inspection on the operation and maintenance of the system to include the hardware or subscription of account. C, MISS shall submit recommendations based on the result of the inspection to TCDS NLT a week after the inspection; and
- e) Prepare requests addressed to the CPNP through the DC for the purchase of equipment and other materials as well as for the maintenance of the PNP SAMS based on the recommendation of C, MISS in coordination with ITMS; and
- f) Perform other tasks as directed.

4) **DC**

- a) Provide funds for the purchase of equipment and other materials needed for the development, innovation, regular operations and maintenance of the PNP SAMS; and
- b) Perform other tasks as directed.

5) **ITMS**

- a) Designated as co-OPR in the implementation of this MC in coordination with the OTCDS;
- b) Provide technical support and expertise in the implementation of this MC;
- c) Responsible for maintaining the day-to-day operations of the PNP SAMS nationwide;
- d) Shall ensure that system security for the PNP SAMS to include audit trails are always checked and reviewed;
- e) Shall provide PES for each PNP personnel using the system if no official email address provided;


CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

- f) Update the PNP offices/units about the necessary licensed operating system and application software of the computers and other patches necessary for the PNP SAMS;
- g) Responsible for providing technical assistance to the PNP offices/units using the PNP SAMS;
- h) Provide basic user training on the user interface of the said PNP SAMS for both operators and executives;
- i) Designate Information Technology Project Officers (ITPOs) as focal persons in the different PNP offices/units responsible for cascading, implementation, maintenance, and user's training; and
- j) Perform other tasks as directed.

6) **D-Staff/P-Staff/PROs/NSUs**

- a) Designate your respective Executive Officers/Chief of Directorial Staff/Chief of Staff as PNP SAMS Supervisor;
- b) Designate your respective Building Commanders as OPR/Administrator to ensure continuous operation of the office/unit PNP SAMS service;
- c) Create, maintain, and deactivate office/unit PNP SAMS accounts upon approval of the Supervisor and create report of the same;
- d) Ensure the system security for the PNP SAMS to include the conduct of regular checking/reviewing of audit trails;
- e) Ensure that only licensed operating system is installed in the desktop computers utilized in the PNP SAMS;
- f) Designate ITPOs in coordination with Camps Commanders, Regional Personnel and Records Management Divisions, and Regional Operations Divisions as focal persons in their respective office/unit responsible for cascading, implementation, maintenance, and user's training of the PNP SAMS;
- g) Ensure technical assistance is provided to the PNP SAMS Users/Operators;
- h) Designate Police Commissioned Officers as PNP SAMS Supervisor who will:
 - (1) Be responsible for the proper, and efficient use of the PNP SAMS to preserve the confidentiality, integrity and availability of the data including its attachments;

CHERRY MAY R PADLA
 Police Lieutenant Colonel
 Administrative Officer

- (2) Use of the designated office/unit PNP SAMS account should be in official capacity and only when authorized by their respective head of office;
 - (3) Be aware of the destructive nature of computer viruses. Trojan horse, worms, and other malicious software (malware). The installation or use of any malicious software using the PNP-owned computer or deployment of such through the PNP network is strictly prohibited;
 - (4) Always take note of the last actions taken before turning over to the next relieving PNP SAMS user/operator and brief the latter about it;
 - (5) Avoid installing games and other software in the office/unit desktop computer intended for the PNP SAMS;
 - (6) Make sure that only licensed or open source software shall be installed in the computer such as the operating system, outlook, office applications, and other programs; and
 - (7) Perform regular preventive maintenance of the desktop computer utilized in the PNP SAMS.
- i) Perform other tasks as directed.

7. PROCEDURES:

The PNP Office ID card to be created and issued, or destroyed and the PNP SAMS System account that needs to be created or deactivated shall be properly communicated to the Administrative Officer and the same shall notify the offices/units PNP SAMS Supervisor prior to deactivation, destruction of any information, whether printed or not, and should be in accordance with the guidelines and procedures set by the Directorate for Intelligence.

8. PENAL CLAUSE:

Any violation of this MC shall be subjected to appropriate administrative sanctions under the provisions of NAPOLCOM MC 2016-002 as amended by NAPOLCOM MC 2019-005.

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.


AUTHENTICATED BY:


CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer

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, Book VII of Executive Order 292 otherwise known as the "Revised Administrative Code of 1987," as amended.




DEBOLD M SINAS
Police General
Chief, PNP

Distribution:
Command Group
D-Staff
P-Staff
D, NSUs
RD, PROs

CPNP Ltrs'20 S084168

S084168

Copy Furnished:
SPA to SILG
LO to OP

AUTHENTICATED BY:


CHERRY MAY R PADLA
Police Lieutenant Colonel
Administrative Officer