MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

GROUP:
19 August 2015

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 1908-12-2015

1. References:

   a. Command Guidance, and;
   b. VAPT and Monitoring Result of Intrusion Prevention System appliance.

2. As per above references, forwarded is the Cyber Security Bulletin number 022 with topic regarding **Philippine Army Network (PANET) Acceptable Usage Policy.**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cyber Security Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
MAJ JOEY T FONTIVEROS (INF) PA Chief, CMB, OG6, PA	6630
RreleaseR'S NAME AND TITLE	
LTCOL JEFFERM PADIGDIG GSC (SC) PA OIC, G6, PA	

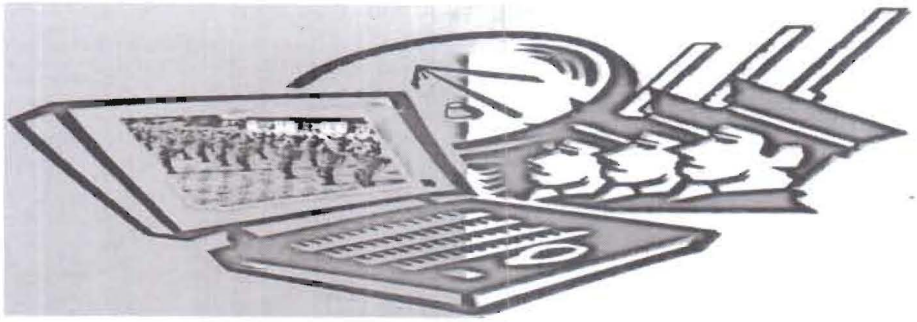
HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB

18 Aug 2015

Cyber Security Bulletin Number: OG6- 022

Philippine Army Network (PA Net) Acceptable Usage Policy



The HPA Local Network Area (LAN) started from a simple computer network with a server and a few stations in CY-1998. It was based on the Institute of Electrical and Electronic Engineers (IEEE) 802.3 Standards or the Ethernet Standards. After several years from the time it was established, it has evolved in a Campus Area Network (CAN) that consists of several servers and hundreds of workstations used by HPA Offices and Post Units.

Use of every aspect of the PA Network is a revocable privilege that should conform to rules and regulations such as:

Acceptable Use

1. Use must be exclusively for the accomplishment of the stated mission and function of the Army.
2. Use must be consistent with the roles appropriate to any network being utilized or accessed.
3. Unauthorized use and/or distribution of copyrighted material is prohibited.
4. Accessing, distributing or storing of threatening or obscene/pornographic material is prohibited.
5. Unauthorized distribution of non-official material is prohibited.

6. Use for private commercial activities is prohibited.
7. Advertisement for external products or services is prohibited.
8. Political lobbying is prohibited.
9. Only work related software is to be downloaded from the Internet to users' workstations.

Netiquette

The Internet community has over the years developed a set of generally accepted guidelines for behavior. This has become known as "Netiquette". Some general principles that should be observed when using both the PA Network and the Internet are:

1. Be polite.
2. Do not use vulgar or obscene language.
3. Use caution when revealing your address or phone number or those of others.
4. E-mail is not guaranteed to be private.
5. Do not intentionally disrupt the network or other users.
6. Users should also follow the 'netiquette' principles of only consuming bandwith especially when downloading or uploading when necessary.

Security

AFP security procedures should be followed. Some common sense practices are as follows:

1. If a security problem is found, notify a system administrator immediately.
2. Do not show or identify a security problem to unauthorized personnel.
3. Do not reveal account passwords or allow another person to use your password. You are accountable for your account.
4. Do not use another individual's password.
5. Any user identified as a security risk will be denied access.

Vandalism

The following as general guidelines as to what can be considered Vandalism and Harassment:

1. Vandalism is defined as any malicious attempt to harm or destroy software or data of another user using the Intranet or other networks. This includes but is not limited to creating or unloading computer virus.
2. Harassment is defined as the persistent annoyance of another user or the interference in another user's work. This includes but is not limited to sending unwanted mail.
3. Vandalism or harassment will result in the cancellation of the offending user's access and the possibility of military or civil disciplinary action being taken.

Malicious Software

1. Users should not intentionally download or copy malicious software from the Internet or other sources.
2. Users should take every precaution to ensure that malicious software is now downloaded or copied from the Internet or other sources.
3. Any software downloaded or copied from the Internet or other sources should be scanned/cleaned using approved antivirus software before being opened or used.
4. If malicious software is detected, the systems administrator should be immediately notified.

Penalties

Users of the PA Network should be aware that such usage is being monitored. Those who violate pertinent rules and regulations such as written AFP policies, AFP Code of Ethics, verbal orders, applicable national and local laws or other official orders will be subject to the following:

1. Immediate revocation of all network access and privileges.
2. Other disciplinary actions including criminal prosecution.

References:

HPA SOP # 03 dtd 03 May 2005
HPA SOP # 12 dtd 23 December 2003
HPA Guidelines on EMCS and Web Publishing dtd 23 December 2003