DEPARTMENT OF THE ARMY
93D SIGNAL BRIGADE (STRATEGIC)
US ARMY SIGNAL NETWORK ENTERPRISE CTR – FORT GORDON
245 O' CLUB DRIVE
FORT GORDON, GEORGIA 30905

REPLY TO
ATTENTION OF

NETC-SFG-DT

26 January 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Network Enterprise Center Violations Policy

1. References:

a. AR 380-67, Personnel Security Program, 9 Sep 88

b. AR 380-5, Department of the Army Information Security Program, 29 Sep 00

c. Privilege Level Access Agreement Best Business Practice, 3 Nov 06

d. DoDD 8500.1, Information Assurance, Certified Current as of 23 Apr 07

e. DoDD 5500.07-R, Joint Ethics Regulation, 29 Nov 07

f. AR 25-1, Army Knowledge Management and Information Technology, 4 Dec 08

g. AR 25-2, Information Assurance, Rapid Action Revision (RAR) 001, 23 Mar 09

h. Acceptable Use Policy, 27 Jan 10

2. IAW the above references, all users utilizing a government system and/or network are required to meet the personnel security standards and receive training prior to gaining access to the device and/or network, and must receive annual refresher training to maintain that access. This policy outlines the prohibited activities as well as the administrative actions to be applied to network access.

3. Prohibited use of Army Information Systems (IS) includes the following:

a. Use of IS that adversely reflects on DoD or the Army such as uses involving sexually explicit e-mail or access to sexually explicit Web sites, pornographic images, or virtual computer-generated or otherwise pornographic images; chain e-mail messages; unofficial advertising, soliciting, or selling via e-mail; and other uses that are incompatible with public service.

b. Use of IS for unlawful activities, commercial purposes, or in support of for-profit activities, personal financial gain, personal use inconsistent with DoD policy, personal use that promotes a particular religion or faith, or uses that violate other Army policies or public laws. This may include, but is not limited to, violation of intellectual property, gambling, terrorist activities, and sexual or other forms of harassment.

c. Political transmissions to include transmissions that advocate the election of particular candidates for public office.

d. Theft or other abuse of computing facilities. Such prohibitions apply to electronic mail services and include, but are not limited to unauthorized entry; use, transfer, and tampering with the accounts and files of others; and interference with the work of others and with other computing facilities.

e. Use of an Army IS that is used for purposes that could directly or indirectly cause congestion, delay, or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with other personnel's use of IS. Such uses include, but are not limited to, the use of IS to:

(1) Create, download, store, copy, transmit, or broadcast chain letters.

(2) "Spam" to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.

(3) Send a "letter-bomb" to re-send the same e-mail message repeatedly to one or more recipients, to interfere with the recipient's use of e-mail.

(4) Broadcast unsubstantiated virus warnings from sources other than systems administrators.

(5) Broadcast unofficial e-mail messages to large groups of e-mail users.

(6) Employ for personal use applications using streaming data, audio, and video; malicious logic and virus development software, tools, files; unlicensed software; games; Web altering tools/software; and other software that may cause harm to government owned computers and telecommunications systems.

4. Forfeiture and Reinstatement of Privileges: Users found in violation of DoD, Army regulations, and/or Network Enterprise Center (NEC) policies will forfeit their network access privileges. Any incident that is criminal in nature will be reported to the Military Police and Criminal Investigation Department. Information Assurance personnel (i.e. IAM/SA/NA/IASO)

found in violation of DoD, Army regulations, and/or NEC policies will also forfeit their IA privileges as outlined in the Privileged-Level Access Agreement. The following administrative actions will be taken when personnel violate IS regulations and policies:

a. 1st Offense – One-week forfeiture of computer/network access privileges and the user must complete the IA awareness training module and test. The certificate must be submitted to the NEC via the unit/organization Commander/Director with an explanation of actions the unit/organization has taken to ensure no further violations will occur.

b. 2nd Offense – Two-week forfeiture of computer/network access privileges and the user must complete the IA awareness training module and test. The certificate must be provided via the unit/organization Commander/Director and NEC to the 7th Signal Command, Designated Approving Authority (DAA) with an explanation of actions the unit/organization has taken to ensure no further violations will occur.

c. 3rd Offense – Permanent forfeiture of computer/network access privileges for the duration of employment in any capacity at Fort Gordon.

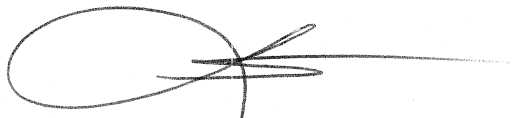
d. The above described actions are not to be construed as the exclusive actions for violators. Supervisors may also consider imposing the full range of adverse and administrative actions, such as those described in AR 25-2, Chapter 1, paragraph 1-5, k (1) and (2).

(1) Sanctions for civilian personnel may include, but are not limited to, some or all of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; suspension with or without pay; loss or suspension of access to IS or networks, and classified material and programs; any other administrative sanctions authorized by contract or agreement; and/or dismissal from employment. Sanctions for civilians may also include prosecution in the U.S. District Court or other courts and any sentences awarded pursuant to such prosecution. Sanctions may be awarded only by civilian managers or military officials who have authority to impose the specific sanction(s) proposed.

(2) Sanctions for military personnel may include, but are not limited to, some of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; and loss or suspension of access to IS or networks and classified material and programs. Sanctions for military personnel may also include any administrative measures authorized by service directives and any administrative measures or non-judicial or judicial punishments authorized by the Uniform Code of Military Justice (UCMJ).

e. Appeals to reinstate computer/network access privileges must be addressed in writing to the 7th Signal Command DAA.

5. The Point of Contact for this memorandum is Ms. Queen D. Harts, Installation Information Assurance Manager, at 706-791-0042 or email: queen.harts@us.army.mil.



LISA E. McCLEASE
Director, Network Enterprise Center-FT Gordon

DISTRIBUTION: A