



DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, US ARMY GARRISON FORT A.P. HILL
18436 4TH STREET
FORT A.P. HILL, VIRGINIA 22427-3114

REPLY TO
ATTENTION OF

IMPH- ZA

1 October 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Commander's Policy Letter #12: Information Technology (IT) Usage

1. Applicability. This policy applies to all military and civilian personnel (including contractor employees) assigned to or working at Fort A.P. Hill, to tenant organizations, which are connected to the Fort A.P. Hill communications infrastructure or Local Area Network (LAN), and to all other persons authorized to use Fort A.P. Hill communications infrastructure and LAN. The communications infrastructure includes all government owned telephones, cell phones, computers, blackberries, personal assistant (PDAS) and the means by which they are connected.

2. Proponent. Information Management Office (IMO), 804-633-8952.

3. References:

a. Department of Defense (DoD) Directive 5500.7-R, Joint Ethics Regulation (JER).

b. AR 25-2, Information Assurance, RAR, 23 March 2009.

c. AR 25-55, The Department of the Army Freedom of Information Act Program, 1 November 1997.

d. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

e. AR 340-21, The Army Privacy Act Program, 5 July 1985.

4. Policy. The DoD JER requires that government resources be used for official and authorized purposes only.

a. Official Business calls are defined as those that are necessary in the interest of the Government (for example, calls directly related to the conduct of DoD business or having an indirect impact on DoD's ability to conduct its business).

b. Authorized uses of communications systems. Authorized use includes **brief local** personal communications from the DoD employee to spouse, checking minor children, scheduling doctor appointment, etc. Such communications may be permitted, provided that they:

IMPH-ZA

SUBJECT: Commander's Policy Letter #12: Information Technology (IT) Usage

- (1) Conform to DoD policy.
- (2) Do not adversely affect the performance of official duties by the employee or the employee's organization.
- (3) Are of reasonable duration and frequency and, when possible, done before or after normal duty hours.
- (4) Are not used for activities related to the operation of a personal business enterprise.
- (5) Do not create significant additional cost to DoD, and does not reflect adversely on DoD. (DoD includes all services and other branches).
- (6) Serve a legitimate public interest, such as furthering the education and self-improvement of employees or improving employee morale and welfare. Employees may also be allowed to conduct job searches in response to downsizing. Using Government computers to send e-mail between deployed soldiers and their immediate family members is authorized.
- (7) Do not overburden the military communication system. Remember, the military communication system (of which the NIPRNET plays a vital part) is designed to support the mission requirements of the Warfighter.
- (8) In accordance with AR 25-2 (Information Assurance) paragraph 4-17, and AR 25-55 (The Department of the Army Freedom of Information Act Program), all external media (floppy disks and CD's) must be marked and controlled according to the classification of the information they contain. Implement media accountability procedures based on the classification of the data. Labeling marking and controlling media are as follows:
 - (a) Unless write-protected or read-only, classify media inserted into a system at the highest level the system is accredited to process until the data or media is reviewed and validated by the Information Assurance Security Officer (IASO).
 - (b) Clear media before reuse in Information System's (IS) operation at the same protection level.
 - (c) Virus scan all removable media before loading it on any computer connected to the Fort A.P. Hill local area network (LAN).
 - (d) Mark and control all media devices, peripherals, and IS's, per AR 25-2 and supplement as follows:
 - aa. TS or SCI or intelligence data per DCID 6/3, DCID 1/7, AR 380-5, and JDCSISSS as applicable.

IMPH-ZA

SUBJECT: Commander's Policy Letter #12: Information Technology (IT) Usage

bb. Classified media per AR 380-5.

cc. FOUO media per AR 25-55.

dd. Privacy act media (sensitive) as FOUO per AR 340-21.

ee. NATO information per AR 380-15.

(e) Mark and control the media or IS after determination of the classification level of the data placed on the media. Implement media accountability procedures based on the classification of the data.

c. Long Distance (toll) Calls. Personal long distance calls are not permitted except in an emergency. A personal long distance call will be:

(1) Charged to the employee's home number or other non-Government numbers (third party call)

(2) Made to a toll-free number;

(3) Charged to the called party if a non-Government number (collect call); or

(4) Charged to a personal telephone calling/credit card.

d. All telephone users must be aware of security issues and their consent to monitoring for all lawful purposes, of restrictions on transmitting classified information over unsecured telephone systems, of prohibitions regarding release of access information such as access codes, and of the need for care when transmitting other sensitive information.

e. Unauthorized uses of communications infrastructure include the following:

(1) Use of communications infrastructure in a way that would reflect adversely on DoD or the Army such as the use of or access to material involving pornography or obscene material (adult or child), copyright infringement, downloading or using peer-to-peer software, gambling, the transmission of chain letters, unofficial advertising, soliciting or selling, and other uses that are incompatible with public service. Participation in Peer-to-Peer activity will result in immediate termination of network connectivity and the user activity will be held responsible for reimbursement of man hours expended for the mitigation and reporting of this vulnerability. Having any type of peer-to-peer file sharing software, such as Gnutella, Morpheus, Kazaa, etc., present on a government system constitutes a poor security practice as it provides a vehicles for authorized and unauthorized individuals to use this system as a platform for searching, transferring or downloading material that may be constituted as improper and/or illicit. These actions violate policy, and may violate local, state, and federal laws. Revealing individual passwords or Common Access Cards pin numbers to other individuals is also prohibited.

IMPH-ZA

SUBJECT: Commander's Policy Letter #12: Information Technology (IT) Usage

(2) Use of communications infrastructure for unlawful activities, commercial purposes or in support of "for profit" activities, personal financial gain, personal use inconsistent with DoD policy, or uses that violate other Army policies or public laws. This may include, but is not limited, to violations of intellectual property, gambling, terrorist activities, and sexual or other forms of harassment.

(3) Leaving a computer logged on and unattended. Users will activate the CTRL ALT- DEL command prior to leaving their workstation.

(4) Political transmissions to include transmissions, which advocate the election of particular candidates for public eye.

(5) Interference. Army communications infrastructure will not be used for purposes that could reasonably be expected to cause, directly or indirectly, congestion, delay or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with other's use of telephone systems. Guidance for telephone calls while at a temporary duty location is reflected in the Joint Travel Regulation (JTR). Abuse of DoD and Army telephone systems may result in disciplinary action.

(6) Wireless. Use of wireless network cards in government owned PCs is strictly prohibited. This prohibition does not apply to official use of tactical wireless assets.

(7) Connecting a personally owned computer to the Fort A.P. Hill LAN.

f. Contractors use of Government communications infrastructure:

(1) Contractors providing resale services related to NAFI operations will use commercial service when available.

(2) Contractors providing appropriated fund type support may receive official service. The Contracting Officer determines if such service is advantageous to the Government and is mission essential. Authorized service must be specified in the contract as Government furnished.

(3) When official telephone service is authorized, Class A service may be provided, as determined by the NEC, contracting officer, or contracting officer's representative for specific contracts.

g. Cellular phones will not be used in lieu of established "wired" telephones. These devices are to be for official business and authorized use only and may be approved for handheld portable use and/or installed in Government vehicles. Official use of these phones will be limited to requirements that cannot be satisfied by other available telecommunications methods and are authorized when warranted by mission requirements, technical limitation, feasibility, or cost considerations. Authorized personal use of cellular phones is subject to the same restrictions and prohibitions that apply to other communications systems.

IMPH-ZA

SUBJECT: Commander's Policy Letter #12: Information Technology (IT) Usage

h. Telephone Control Officer's (TCO) must certify all bills for their activity and return to NEC. Original signature is required.

i. Telephone Control Officer's will recover phone charges, as practical, for unauthorized personal telephone calls placed on official telephones by personnel in their organizations. Persons making unauthorized telephone calls may be subject to disciplinary action as well as charged for these calls.

5. Point of contact for this policy memorandum is Louis Scott, Chief, Information Management Officer, extension 8952.



PETER E. DARGLE
LTC, AR
Commanding

DISTRIBUTION:

A