DEPARTMENT OF THE ARMY
UNITED STATES ARMY STUDENT DETACHMENT
5450 STROM THURMOND BOULEVARD ROOM 244
FORT JACKSON, SOUTH CAROLINA 29207

ATMT-LTB-SD 25 October 2017

MEMORANDUM FOR All personnel permanently assigned and/or attached to the United States Army Student Detachment (USASD)

SUBJECT: Policy Memorandum #28 – **USASD Computer Use Policy**

1. This memorandum provides consolidated guidance for the use of the USASD Information Systems (IS) including, but not limited to: computers, software applications and related office automation equipment and the ramifications of misuse. This memorandum applies to all military, civilian, and contract employees of the USASD.

2. Access to all government information systems and networks are for official use only and authorized purposes as set forth in references: DOD 5500. 7-R, DOD Joint Ethics Regulation (JER); AR 25-1, Army Information Management; AR 25-2, Information Assurance; AR 380-53, Information Systems Security Monitoring; AR 690-700, Personnel Relations and Services; Manual for Courts-Martial, 2002 Edition.

3. Use of the Fort Jackson network constitutes consent to monitoring. Users should be aware that information placed on a government system becomes the property of the government. Users have no expectation of privacy except as outlined in references: Army Information Management; AR 25-2 and Information Systems Security Monitoring; AR 690-700.

4. Responsibilities.

a. The USASD Commander is responsible for Information Assurance for the unit. Information Assurance Security Officers (IASO) and Information Management Officers (IMO) will be appointed to ensure USASD personnel adhere to IS policies.

b. The IASOs and the IMOs will ensure this policy is understood and followed by all USASD employees within his/her area of concern. All personnel who are witness to unauthorized use of Computers will report the following: all real or suspected incidents of policy violations through the chain of command to the Directorate of Information Management (DOIM), Information Assurance Manager (IAM). Ensure that all workstations are configured for Security Update Server (SUS) for Information Assurance Vulnerability Alert (IAVA) compliance and DOIM Norton Anti-Virus {AV) Server for updates.

c. Supervisors are responsible for enforcing proper use of government information systems by their subordinates. Supervisors may revoke the authorized personal use, or parts thereof, for misuse of services for any reasonable or just cause. They may authorize employees to use government information systems for limited personal use so long as the personal use does not violate this policy or requirements of references. Report all real or suspected incidents to the appropriate IASO/IMO. Personnel are responsible for updating the Annual Security and Cyber Awareness Challenge to maintain Fort Jackson network access.

d. Users of the Fort Jackson network services have permission to use these services for official use only or for personal use if the personal use meets the requirements of this policy and references. Users are completely responsible for the use of system services under their system account (i.e., USERID/Password). Users should report real or suspected incidents of policy violations to his/her supervisor. Users have permission to access other than government Internet and e-mail resources for professional development, research, and educational purposes.

(1) If not part of official duties, users should perform personal activities before and after work hours, during lunch periods and other authorized breaks during the work day.

(2) This permission does not extend to personal communications to solicit business, advertising, or other selling activities in support of a personal business enterprise, any other use that would reflect adversely on the government or which is incompatible with public service.

e. Contractor personnel operating under service contracts with the Directorate of Contracting or other federal agencies are authorized use of the Fort Jackson Network services to the extent agreed upon in the contract.

5. Policy.

a. **Inappropriate use of the Fort Jackson network services can, and may, result in disciplinary action, to include adverse administrative actions or judicial measures being taken against users of such services.**

b. Users must possess the required favorable security investigation (for unclassified access) in lieu of a security clearance and must read and sign the Fort Jackson Acceptable Use Policy (AUP). Signed statements for each user must be kept on file for as long as the user has access to network services. This policy also requires annual IA refresher training. Reviewing the Acceptable Use Policy at annual counseling or viewing IA Videos/CDs are two ways to accomplish the annual requirement. Employees may resign the AUP to verify training completion.

c. For the purposes of this policy, **"authorized personal use"** includes use as authorized by this memorandum or as specifically authorized by supervisors using

guidelines issued under this memorandum and references. Examples of approved personal use are:
(1) Sending e-mail to their children studying at a university, sending e-mail to their Families at home while on temporary duty; making a medical appointment; authorizing a financial transaction; etc.

(2) Sending or receiving personal e-mail if it is comparable to a personal telephone call and the use is no more disruptive than a telephone call and does not result in additional cost to the government.

d. The use of government computers, software and networks to transact e-mail, share files or to access the Internet must be for-official use only or for authorized personal use when it serves the best interest of the USASD, Fort Jackson, and the United States Army.

e. Passwords must be protected always. Passwords must meet the criteria in reference 4d and will be used by the account holder only (i.e. NO SHARING).

f. Only authorized hardware and software will be used on government IS. Personally owned software, freeware, shareware or another public domain software will not be loaded on USASD IS.

g. Anti-virus software will be loaded on all USASD IS and kept at the most current level. All networked work stations must be configured to automatically update AV from the DOIM AV Server. All diskettes, compact disks, and attachments will be scanned for viruses before any information is down loaded to an IS.

h. Classified information will not be introduced to unclassified IS.

i. IS **will not** be altered, changed, or reconfigured from the Fort Jackson Base line for the IS nor will executable codes (such as, but not limited to, .exe, .com, .vbs, .bat files) be introduced to any IS without specific authorization from the OHR.

j. USASD users **will not** participate in the writing and dissemination of malicious code.

k. IS **will not** be used for commercial financial gain or illegal activities.

l. Users **must** utilize screen locks and/or log off the system when departing the area even for short periods of time.

m. All suspicious emails, files, short cuts, or system problems **must be** reported to your IASO/IMO and up through the chain of command.

n. Address all questions regarding this policy, responsibilities, or duties to your IASO/IMO.

o. The following activities are **NOT** acceptable uses of USASD IS:

(1) **Advertise** or solicit for sale of personal property or services.

(2) Announce or **endorse private enterprise fund raising** or participate in any activity for personal gain.

(3) Engage in **unethical** activity (i.e. spam, profanity, sexual content, gaming, pornography or any other form of unlawful activity via email, the Internet or file sharing service.

(4) Establish unauthorized services (i.e. peer-to-peer (P2P), distributed computing). Some examples of P2P are Kazaa, Morpheus, and Gator but there are many others. Typically these services load to an IS and then allow others to access the hard drive through the internet.

(5) Engage in any activity that would interfere with official duties, undermine readiness, or reflect adversely on the USASD, Fort Jackson or the U.S. Army.

(6) Use email accounts to distribute **chain letters, computer hoaxes** or **any form** of unofficial mass mailing or make public any information that falls under the Freedom of Information Act or Privacy Act.

(7) Engage in any activity that uses excessive band width, including but not limited to, data streaming services such as stock market services, weather updates, web shots (live pictures), Internet radio and TV broadcasts, and on-line games.

6. Point of contact for this memorandum is the undersigned at (803) 751-5305.

PEACH.ALEJANDR
A.DEL
RELLO.1238465458

Digitally signed by PEACH.ALEJANDRA.DEL
RELLO.1238465458
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=USA, cn=PEACH.ALEJANDRA.DEL
RELLO.1238465458
Date: 2018.02.28 14:17:43 -05'00'

ALEJANDRA D. PEACH
CPT, AG
Commanding