DEPARTMENT OF THE ARMY
UNITED STATES MILITARY ACADEMY
WEST POINT, NY 10996

MACC-O

21 September 2016

MEMORANDUM FOR the United States Corps of Cadets, West Point, NY 10996-1692

SUBJECT: Policy Letter #17: Information Technology Standards for the Corps of Cadets

1. Purpose. The purpose of this memorandum is to provide guidance for the Cadet use of computers, network resources, application software and operating systems. Use of government network systems, including e-mail systems, constitutes consent to monitoring. This policy is punitive. Violations of the standards set herein are punishable under the Uniform Code of Military Justice, Article 92, *Failure to Obey Order or Regulation*, and under the Cadet Disciplinary System under the provisions of Army Regulation 210-26, *United States Military Academy*, Chapter 6-17.

2. Cadet issued computer. Cadets are required to maintain a personal computer system in working order. This must be the Cadet's issued system or an issued replacement from subsequent Cadet issued systems.

a. Replacement Computers. The Cadet's TAC and the Chief of Goldcoats may approve replacement computers in writing prior to acquisition. A Cadet may only place an IETD procured system on the network. A justification of damages and a detailed list of all requested hardware and software specifications must be identified on the memorandum. A replacement computer must meet the minimum standards of the class issued computer. The only authorized operating system for a replacement computer is the class issued operating system with the same privileges as the class.

b. Modifications of Issued Computer. All hardware modifications will be approved by the Chief of Goldcoats prior to acquisition to ensure consistency with the computer's warrantee.

c. Operating Systems. The only approved operating system for Cadet use on the USMA network is the class issued operating system. Cadets are not authorized to remove their issued operating system and install a replacement operating system. A Cadet is not authorized to modify their user privileges, or adjust their profile to gain privileges other than those authorized. Authorization to run any other operating system or modifying their privileges will be granted in writing by a Staff & Faculty member and the Chief of Goldcoats. Authorization will only be granted for academic purposes.

3. Software Copyright Compliance. Cadets are responsible for ensuring they are in compliance with the copyright restrictions for each piece of software they maintain on their computer systems. Cadets are not authorized to use or place any software on their personal computer for which they do not have copyright authorization, nor will they make, or permit to be made, copies of the software, either for their use or for another Cadet's use; unless this is explicitly authorized in the software's copyright conditions. The copyright conditions for commercial (issued and Cadet-purchased) software are normally stated in writing within the software's published documentation. The copyright conditions for shareware (software for which a fee is requested or expected) and freeware (software offered free of charge) are normally included in the software's distribution as "read-me" or similar files. Cadets must read and adhere to the copyright restrictions for shareware and freeware just as for commercial software. Cadets are not allowed to use or possess software key generators, password cracking applications, or copyright cracking applications.

4. Network Connectivity Requirements. All Cadets will maintain an active connection to the USMA network. The Cadet Training and Support Branch (Goldcoats) will support only hardware procured through IETD Cadets are responsible for obtaining hardware and software assistance from the Goldcoats or their ISO to ensure full and continuous connectivity to the USMA data network.

5. Remote Access to the USMA Network. Cadets are authorized to employ VPN technology deployed by IETD to access the USMA network while not at USMA. The IETD supplied VPN client is the only remote access application authorized. Cadets will not install or use hardware or software designed to allow remote users access to any computer, network device, or file share. Exceptions to this policy are granted by the Dean's Information Assurance Manager.

6. Computer Virus Protection. All Cadet computer systems will include the appropriate anti-virus software made available through the Goldcoats. No other anti-virus software is authorized for use. This software will be active on the computer at all times. Cadets may not disable this software or remove it from their systems. Cadets will use the anti-virus software as directed to scan all software/files introduced into their system, to include products loaded via removable disk and over the data network. Cadets will ensure their computers receive updates from the USMA anti- virus corporate servers first and the vendor definition servers second.

7. Electronic Mail. The USMA Exchange mail system allows for quick and accurate dissemination of message traffic among Staff and Faculty and the Corps of Cadets. Cadets are not authorized to auto-forward email from a USMA account to any non-Department of Defense email server. All use of email is required to adhere to standard

customs and courtesies for military professional correspondence in accordance with AR25-50.

8. Network Material. The USMA data network is the property of the U.S. Government. Any/all material placed onto or transmitted via the network is subject to monitoring by system administrators. The login banner/discloser provides the most up to date legal authority for monitoring of DoD information assets.

a. Network Presence. Under a network-operating environment, Cadets appear in the global list of network users and are able to connect to other computers to share files across the network. All Cadets who have a network presence will maintain this presence in accordance this policy. Cadets will not modify the computer name without written authorization from the Chief, Goldcoats.

b. File and Directory Sharing. Cadets are responsible for controlling outside access to their drives and files. Cadets may share directories to other USMA personnel, but will ensure that each shared directory resource is properly protected. No Cadet may access another PC without the express and prior approval of that PC owner. A Cadet may not set permissions for free access by everyone to his or her drives and files, i.e. access must be limited to users that the PC owner specifically designates. No copyrighted software (e.g. games, MP3's, Movies, etc) will be shared over the network unless the copyright specifically grants free and unrestricted distribution.

c. Travel Folder. Cadets' common access cards have a travel folder integrated with the user. Cadets may use the folder for storage of confidential information they wish to keep secure.

9. Appropriate Use. Cadets are afforded the same access to computing and networking resources as faculty and staff. These resources must be used for educational purposes and to carry out the legitimate business of the Academy. Cadets must practice considerate and responsible computing and adhere to common sense standards to determine appropriate use of academic computing resources. Any activity that obstructs or hinders the authorized use of USMA academic computing and network resources is prohibited. Cadets are authorized to play a game across the network only on the authorized operating system. At anytime, the chain of command and/or network administrators reserve the right to revoke this privilege as a result of adverse impact to the network or good order and discipline. Games that use Peer to Peer (P2P) protocols are prohibited unless the P2P function can be disabled.

10. Inappropriate Use. Cadets will not display or store any pornography or sexually related materials on their computers at any time. Cadets are expressly forbidden from accessing, via any computer system operated by the government, any website that

contains pornographic material. A warning screen will be displayed when a user attempts to access a web site that may be unauthorized, as identified by the Academy's monitoring software. Additional examples of inappropriate activities include (but are not limited to):

a. Installing or maintaining network servers (file server, domain server, web/chat server, game server, etc.) of any kind.

b. Breaking into a system, server, or personal computer and / or accessing data files and programs without explicit permission or authorization. An open file share or incorrectly secured file does not constitute authorization for access.

c. Releasing a virus or other program that disables system performance or hinders other clients.

d. Exploiting security gaps.

e. Hindering supervisory, maintenance or accounting functions of the systems.

f. Tapping phone or network lines.

g. Monopolizing computer resources or computer access.

h. Obtaining, possessing, using, or attempting to use someone else's user account or password.

i. Sending email, instant messages, or any other electronic communication from another users account.

11. Harassment. Harassment in any form and for any reason is unacceptable behavior and is not tolerated. With regards to computers, networks, and social media, the following will not be tolerated:

a. Sending unsolicited e-mail, junk mail, or propagating chain letters.

b. Using academic computing resources to engage in ethnic, racial, or sexual harassment of another person.

c. Communicating a threat to another person or organization.

d. Inappropriate Items. Cadet will not display or store any pornography, racial, ethnic, or sexually related materials on their computers at any time.

12. Inappropriate Use of Electronic Mail Services. The only authorized email service is the USMA Exchange mail system. Cadets may not use anonymous e-mail services to transmit or receive electronic mail. The USMA Exchange Mail services may not be used in a manner that overburdens network telecommunications systems. Cadets should not send e-mail that could reasonably be expected to cause excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of e-mail services. Such interference includes, but is not limited to, the use of e-mail services to:

a. Sending email chain letters.

b. Spamming by exploiting distribution lists to provide widespread distribution of unsolicited email.

c. Broadcast of unnecessary advertisements, personal announcements, daily quotations, jokes, or similar transmissions.

d. Letter bombing by sending the same e-mail repeatedly to one or more recipients to interfere with the recipient's use of e-mail or the servers' ability to adequately handle message traffic.

e. Broadcast of unsubstantiated virus warnings from sources other than USMA systems administrators.

f. Directing messages to large audiences and sending repeats of the same messages as "reminders."

g. Forging or ghostwriting electronic messages. Creating, altering, or deleting the attribution of origin to intentionally mislead the recipient as to the author of an electronic communication.

13. The point of contact for this memorandum is the Brigade Senior Enlisted Advisor at 845-938-7904.

BRIAN J. REED
COL, IN
Brigade Tactical Officer