DEPARTMENT OF THE ARMY
UNITED STATES MILITARY ACADEMY
West Point, New York 10996

REPLY TO
ATTENTION OF

MAIO

USMA POLICY MEMORANDUM #25-IA-02-08

SUBJECT: Peer-to-Peer Software Use.

1. **PURPOSE.** To establish West Point policy prohibiting the use of peer to peer software (P2P) on the West Point network.

2. **REFERENCES.**

a. AR 25-1, Army Information Management, 31 May 2002

b. AR 25-2, Information Assurance, 3 August 2007

c. USMA MOU with CIO/G6, dated 12 June 2007

d. USCC SOP and USCC 351-2

3. **APPLICABILITY.** This policy applies to all users on the West Point Local Area Network (LAN) including staff, faculty, cadets, contractors, authorized visitors, and other personnel of the United States Military Academy, United States Army Garrison West Point, and tenant and supported activities thereof.

4. **BACKGROUND.** P2P software introduces unacceptable risk to all users of local area networks where it is being used. P2P software enables the sharing of information between users via unsecure means and sometimes without the user's knowledge. Programs such as Skype and Limewire make direct connections between individual computers and allowing vulnerabilities to be passed from one to another. The vulnerabilities found in P2P software introduce unacceptable risks to our networked environment.

5. **POLICY.**

a. All software using P2P technology is prohibited. Exceptions to the policy must be approved in advance by the Designated Approval Authority (DAA) for the West Point LAN. All submissions requesting the use of a P2P application should include a description of the software, intended use of the application and justification explaining why P2P software is the only solution to meet the requirement. The requesting activity must submit their documentation to the appropriate Information Assurance Manager (IAM) for review. If the request is deemed valid by the IAM it will be forward to the Configuration Control Board (CCB) for processing. The final approval authority is the Designated Approval Authority for the West Point LAN. A list of any approved exceptions to this policy will be posted on West Point internal websites.

b. The Office of the Chief Information Officer (OCIO) will maintain a list of known prohibited P2P applications and P2P plug-ins and post it on their internal website. This provides users, with an easily accessible reference to help them avoid the use of these prohibited software products and comply with this policy.

c. Asset discovery tools designed to identify use of prohibited software will be used by IA personnel to insure compliance. Removing or disabling these tools on any workstation or server is a violation of this policy.

d. First Offenses:

(1) Cadets:
Cadets suspected of having prohibited P2P software on their laptop will be directed to report to the Goldcoats, IETD. If the presence of P2P is validated by the Goldcoats, the cadet's computer will be re-imaged IAW AR 25-2 and the cadet will be directed to remove any files downloaded or associated with the application. If the software was on the prohibited list, the cadet will forfeit local administrator permissions on the laptop for a period of one month. IETD will submit a Cadet Activity Report (COR) as the method for providing notification of the policy violation to the cadet's chain of command. Cadets that do not report to IETD (Goldcoats) within three business days or coordinate for an exception once they are notified of a possible violation will have their USMA computer account disabled until remediation is completed as detailed above. IETD will notify the cadet's Chain of Command when the cadet has not reported within the 3 business days. The TAC officer will be able to request an extension for operational reasons, as necessary. CORs will be processed in accordance with USCC SOP and USCC 351-2 Cadet Disciplinary System.

(2) All Others:
Personnel suspected of having prohibited P2P software on their computer will be directed to report to the IT support organization for their activity. If the presence of P2P is validated, the computer will be re-imaged IAW AR 25-2 and the system owner will be directed to remove any files downloaded or associated with the application. If the software was on the prohibited list, the user will forfeit local administrator permissions on the system for a period of one month. The IAM will notify the user and the activity or departments IMO or DCO. Department heads or Activity Directors can provide an exception to the loss of system administrator privileges on an individual basis. If a staff, faculty, garrison or tenant user does not attempt to resolve the issue with their activity IMO or DCO within 3 working days, the IAM will notify the user's organization director/department head.

e. Second Offenses:

(1) Cadets:
Cadets will be required to report to IETD (GoldCoats) within three working days to validate the presence of unauthorized P2P software. If it is determined to be a valid and willful second time offense, the computer will be re-imaged in accordance with AR 25-2, and the cadet will have their system administrator privileges removed for a period of six-months and a COR will be submitted to the cadets TAC officer. Cadets that do not report to IETD (GoldCoats) within three business days once they are notified of a possible violation will have their USMA computer account disabled until remediation is completed as detailed above. IETD will notify the cadet's Chain of Command when the cadet has not reported within the 3 business days. The TAC officer will be able to request an extension for operational reasons, as necessary. CORs will be processed in accordance with USCC SOP and USCC 351-2 Cadet Disciplinary System.

(2) All Others:

After the appropriate validation steps, the computer will be rebuilt IAW AR 25-2. If it is determined to be a valid and willful subsequent offense, the individual involved will be referred to their chain of command for appropriate disciplinary action. Continued violation of the policy will be considered serious in nature and will be forwarded to the Activity Director or Department Head for administrative actions. If a staff, faculty, garrison or tenant user does not attempt to resolve the issue with their activity IMO or DCO within 3 working days, the IAM will notify the user's organization director/department head.

f. Subsequent Offenses: For all subsequent offenses users will lose their local administrative rights for a period of one year. A cadet that will be away from West Point for an extended period may apply to have permissions reinstated during that period of time. Upon return to West Point the cadet must immediately notify IETD (Goldcoats) to disable local administrative permissions. Failure to report to Goldcoats, IETD upon return can result in the cadet's computer account being disabled. IETD will work with the cadet's chain of command to resolve any issues with cadets and the status of their compliance with this policy

6. **RESPONSIBILITIES.**

a. All supervisors will:

(1) Educate their personnel on P2P vulnerabilities and ensure users are aware of and fully understand this policy.

(2) When notified, provide assistance to Information Assurance personnel investigating potential violation of this policy.

(3) When validated, take appropriate steps to counsel, retrain or reprimand personnel in violation of this policy, as appropriate.

b. IETD will:

(1) In conjunction with USCC S-6 will be responsible for educating cadets on the P2P policy and the implications of creating a vulnerability to the network at the beginning of each year.

(2) Notify cadets, and Staff and Faculty users (as appropriate) along with the TACs, DCOs, or IMOs of P2P incidents and execute the requirements in paragraph 5d, 5e or 5f.

c. Activity IAMs will:

(1) Ensure computers found with P2P software are rebuilt IAW AR 25-2.

(2) Validate proper rebuild by running the Regional Computer Emergency Response Team (RCERT) Rebuilt Verification Tool (RVT).

(3) Forward RVT results to the DOIM Information Assurance Security Office.

(4) Provide guidance to supervisors to assist in determining the proper actions for users found with P2P software on their computers.

d. All Information Management Officers (IMOs), and Department Computer Officers (DCOs) will:

(1) Ensure that users in their activity understand this policy.

(2) Assist the activity IAM in the validation of P2P software on a user's computer and if verified, rebuilding of the computer.

e. DOIM will:

(1) Notify activity IAMs or IMOs of the presence of P2P software on computers within their area of responsibility so they can complete the task of validating the presence of P2P software.

(2) Provide guidance to activity IAMs on actions required for rebuilding computers IAW AR 25-2.

(3) Conduct periodic scanning of the West Point LAN to determine compliance and provide scan results to the appropriate activity IAM.

7. **EXPIRATION**. This policy is effective until superseded or rescinded.

FOR THE SUPERINTENDENT:

MICHAEL COLPO
COL, IN
Chief of Staff

DISTRIBUTION
A-E Electronic