



DEPARTMENT OF THE ARMY  
UNITED STATES ARMY ROTC BATTALION AND INSTRUCTOR GROUP  
UNIVERSITY OF ILLINOIS AT CHICAGO  
728 West Roosevelt Road  
Chicago, Illinois 60607-4920

Effective 18 July 2002  
As Revised 10 Mar 2005

## **COMPUTER USE POLICY**

**PURPOSE:** As part of this organization's commitment to the utilization of new technologies, all personnel have access to the internet. In order to ensure compliance with copyright law and protect us from being victimized by hacking and malicious viruses, the following is effective upon receipt of this policy:

It is the University of Illinois and US Army Cadet command policy to limit internet access to Official Business. Members of this command are authorized to access the internet for personal use after business hours in strict compliance with the other terms of this policy. The introduction of viruses or malicious tampering with the computer system is strictly prohibited. Any such activity will result in disciplinary action.

### **User Responsibility**

- **Login Responsibility:** I understand that this account is for my sole use and I will not disclose my password. I accept full responsibility for any activity that occurs under my login.
- **Limitations on Access:** Under the provisions of 18 U.S.C. § 1030 as amended ( The National Information Infrastructure Protection Act of 1966) (a) Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains – (b) Information from any department or agency of the United States may be subject to fines up to \$10,000 and or imprisonment for up to 10 years.
- **Consent to monitoring:** This system will be monitored to ensure information security, system integrity, and the limitation of use to official purposes. The use of DOD computer systems constitutes consent to monitoring. Access and network traffic logs are screened regularly for system misuse.
- **Right to terminate accounts:** The ISSO or IT Manager may terminate account access without warning, as deemed necessary to ensure security and integrity of information systems.
- **Locked accounts:** Prior to the ISSO unlocking a user account, counseling must be completed and user policy must be reviewed and completed.

### **UNDERSTAND THE FOLLOWING:**

- You leave your network identification at every website you visit. Your use of any Government system constitutes agreement to monitoring. Remember that access logs are being screened regularly.
- Every file downloaded from the internet must be scanned with current (Within 10 days old) Virus definition (dat) files.

---

**Initials**

**UNDERSTAND THE FOLLOWING: (Continued)**

- Web surfing to Lewd or pornographic web sites and downloading such material is prohibited and subject to punishment under the UCMJ and other Federal and state laws
- Truth or accuracy of information on the internet or received e-mail must be corroborated by a separate (Reliable) source.
- Battalion members and cadets authorized access to Battalion Hardware shall not place company material (copyrighted software, internal correspondence, etc) on any publicly accessible computer without IMO permission.
- Alternate Internet service provider (ISP) connections to Battalion internal network are not authorized.
- The internet does not guarantee the privacy and confidentiality of information. Know and understand that sensitive material transmitted over the internet may be at risk of detection by a third party.
- Unless otherwise noted, all software on the internet should be considered copyrighted work. Therefore, you are prohibited from downloading software and or modifying such files without permission of the copyright holder. Any such infringing activity by you may become the responsibility of this organization. We then under the provisions of 18 U.S.C. § 1030 have the option of holding you criminally liable for your actions.
  - Software will be utilized within the scope of the license agreements.
  - Software will be provided to each station on the Battalion Subnet. All software added by the user must be approved by the unit IT manager prior to installation. Software introduced at your station without prior consent will be subject to removal without notice and subject the user to disciplinary action.
  - Unauthorized copies of software made for the purpose of distribution will not be tolerated in this organization. Any person illegally reproducing such software will be subject to both civil and criminal penalties including fines and imprisonment. Access to publicly accessible computers will be terminated.
  - Each computer user is further advised not to loan, distribute or copy software for student, clients or vendors under penalty of law.
  - Software will be procured through normal logistics channels. Users who feel that misuse of software has occurred will contact the IT manager / IMO and report any violations.
  - **Downloading music or other copy right protected media is prohibited under applicable laws.** You may not participate in any file share venture involving downloading from third parties or services. Such conduct will be cause for termination of network privileges and disciplinary action under the UCMJ and other federal statutes. You are also placed in jeopardy of civil litigation as a result of this inappropriate pirating of music/software or copyrighted material

I have read the Computer Use policy. I further understand that a violation of any of the provisions indicated above may subject me to disciplinary action under the UCMJ in addition to civil and criminal prosecution under the provisions of 18 U.S.C. § 1030 as amended (The National Information Infrastructure Protection Act of 1966).

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Initials