

## METC STUDENT ACCEPTABLE USE POLICY (AUP)

*The purpose of this policy is to outline the acceptable use of computer equipment within a DoD organization. These rules are in place to protect the employee and the organization. Inappropriate use exposes DoD network users to risks including attacks, compromise of network systems and services, and legal issues. This policy applies to all students, employees, contractors, consultants, temporary employees, and other workers assigned to the DoD organizations.*

1. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained on the network from unauthorized or inadvertent use, modification, disclosure, destruction, and denial or service.
2. **Access.** Access to this network is for official use and authorized purposes and as set forth in DOD Directives 5500.7-R (Joint Ethics Regulation) AR 25-2 (Information Assurance) and Army network policy.
3. **Revocability.** Access to METC Information Systems resources is a revocable privilege and is subject to content monitoring and security testing.
4. **Unclassified information processing.** The NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information only. No information with a classification higher than UNCLASSIFIED, SENSITIVE shall be used or stored on any computer system or network at METC.
5. **Public Key Infrastructure (PKI) Use:** Public Key Infrastructure provides a secure computing environment therefore the Common Access Card (CAC) will be used for all network access to METC systems.
6. **User Minimum-security rules and requirements.** As a network system user, the following minimum-security rules and requirements apply:
  - a. I understand personnel are not permitted access to the network unless they have met the appropriate DOD and METC security requirements for accessing the system.
  - b. I will complete the required security awareness-training (Annual AT Awareness Training Level I or Computer Security for Users) and provide proof of completion to my IASO. I understand that my account will be disabled if I do not complete the annual certification training by the required date.
  - c. I will protect my logon credentials (passwords, pass-phrases, PIN numbers) at all times.
  - d. When I use my CAC to logon to the network, I will ensure it is removed and I am logged off prior to leaving the computer
  - e. I will use only authorized hardware and software on the DoD network to include wireless technology. I will not install or use any personally owned hardware (including removable drives), software, shareware, or public domain software.
  - f. To protect the systems against viruses or spamming, I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb storage device, or other storage media.
  - g. I will not attempt to access or process data exceeding the authorized IS classified level.
  - h. I will not alter, change, configure, or use operating systems, programs, or information systems except as specifically authorized.
  - i. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

j. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

k. I will not utilize METC or DOD provided IS for commercial financial gain or illegal activities.

l. Maintenance will be performed by the System Administrator (SA) only.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the SA and/or the Information Assurance Security Officer (IASO) and cease all activities on the system.

n. I will address any questions regarding policy, responsibilities, and duties to my IASO and/or the METC Information Assurance Manager (IAM).

o. I understand that each Information System (IS) is the property of the METC and is provided to me for official and authorized use.

p. I understand that monitoring of the network will be conducted for various purposes and information captured during monitoring may be used for possible adverse administrative, disciplinary or criminal actions. I understand that the following activities are prohibited uses of any DoD IS:

- (1) Unethical use (e.g. Spam, profanity, sexual misconduct, gaming, extortion).
- (2) Accessing and showing unauthorized sites (e.g. pornography, streaming videos, E-Bay, chat rooms).
- (3) Accessing and showing unauthorized services (e.g. peer-to-peer, distributed computing).
- (4) Any use that could cause congestion, delay, degradation or disruption of service to any government system or equipment is unacceptable use (e.g., video, sound or other large files, "push" technology on the internet and other continuous data streams).

q. By signing this document, I acknowledge and consent to the following conditions when I access Department of Defense (DOD) information systems:

- (1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct, law enforcement (LE), and counterintelligence (CI) investigations.
- (2) At any time, the U.S. Government may inspect and seize data stored on this information system.
- (3) Communications using data stored on U.S. Government information systems are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
- (4) This information systems includes security measures (e.g., authentication and access controls) to protect U.S. Government interests; not for my personal benefit or privacy.

\_\_\_\_\_  
Directorate/Division/Branch/Course

\_\_\_\_\_  
Date

\_\_\_\_\_  
Last Name, First, MI (print)

\_\_\_\_\_  
Rank/Grade

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Area Code and Phone Number