US Army Logistics University
Fort Lee, VA
Acceptable Use Policy (AUP) – Students

This policy must be signed and returned to Room B133. Failure to do so will result in the denial of access to all network resources.

1. Understanding. By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

a. You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

b. You consent to the following conditions:

(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 (PM), 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, or data stored on, this information system 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 system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

(5) Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(a) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(b) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(c) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(d) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

(e) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized

to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(f) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(6) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

(7) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind users of conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

2. Access. Access to the Fort Lee Installation Campus Area Network (FL ICAN) is only for official use and for authorized purposes and as set forth in DOD 5500.7-R “Joint Ethics Regulation” or as further limited by this policy.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified information processing. The Secret Internet Protocol Routing Network **(**SIPRNET) is the primary network approved to process SECRET collateral information. The Fort Lee SIPRNET Installation Campus Area Network (FL SICAN) is a US-only system and is authorized for SECRET or lower-level processing in accordance with accreditation packages, identification, etc. The release of TOP SECRET information through the SIPRNET is a security violation and will be investigated and handled as a security violation or as a criminal offense. SIPRNET users will sign a separate AUP.

5. Unclassified information processing. Non-Secure Internet Protocol Router Network (NIPRNET) is the primary unclassified information system for the FL ICAN. It is also a US-only system. NIPRNET provides unclassified communication to external DOD and other United States Government organizations. Primarily this is done via electronic mail and Internet networking protocols. NIPRNET is approved to process UNCLASSFIED, SENSITIVE information in accordance with AR 25-2. The NIPRNET and the Internet are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.

6. Minimum security rules and requirements. Personnel are not permitted access to SIPRNET and NIPRNET unless in complete compliance with Army personnel security requirements as prescribed in AR 25-2. As a NIPRNET and/or SIPRNET system user, the following minimum security rules and requirements apply:

a. I understand that I have the primary responsibility to safeguard the information contained in the Fort Lee Installation Campus Area Network (ICAN) from the unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

b. I will complete all user security awareness-training offered by this organization before system access is granted. I will participate in all new and future training programs as required (inclusive of threat

identification, physical security, acceptable use policies, malicious content and non-standard threats such as social engineering, etc.).

c. I will protect passwords or pass-phrases. Student passwords will be given out by the Course Director and I will not attempt to change it. I will not share my password or CAC PIN with anyone else. If I know my CAC is compromised, I will obtain a reset and report any password compromise to an SA.

d. I will use only Government provided hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software. I will not load or import any software without the written approval of the IASO.

(1) Wireless capabilities on all personally owned wireless equipment (PDAs, cell phones, Blue Tooth devices, & notebook computers) will be disabled. Under no circumstances will these devices be allowed to function within ALU with its wireless capabilities turned on.

(2) **All thumb drives, both government and personally owned, are prohibited** and will not be attached to Government computers, per the Direction of Army NETOPS (Network Operations), 17 Nov 2008.

e. I will immediately report any suspicious output, files, unauthorized software shortcuts, or system problems to my Course Director and cease all activities on the system.

f. I will use virus-checking procedures before uploading or accessing information from any system diskettes, attachments, or compact disks. I will report any antivirus alerts or notifications immediately to my Course Director. I will stop using the system until given instructions by my Course Director.

g. I will not attempt to access or process data exceeding the authorized classified level.

h. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

i. I will not run “sniffers” (utilities used to monitor network traffic, commonly used to spy on the network user and attempt to collect their passwords) or any hacker-related software on my government Computer (GC), IT system, or network.

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 Army- or DOD- provided ISs for commercial financial gain or illegal activities.

l. I acknowledge that only the security-trained System Administrator (SA) or authorized representative will perform system maintenance or troubleshooting.

m. I will log off the workstation when departing the area.

n. I will address any questions regarding policy, responsibilities, and duties to the organization IASO.

o. I will not connect any personal IT equipment to my GC or to any Government network without the written approval of my commander, SA, or IASO and the DOIM. This includes any personal computers, digitally enabled devices, personal electronic devices, personal digital assistants (e.g. palm pilots, smart phones, personal Blackberry devices, iPods, mp3 players).

p. I will not use Internet “chat” services (for example, AOL, MSN, Instant Messenger, Yahoo) from my GC. If chat service is needed, I will use my AKO account.

q. I also understand that the following activities define ***unacceptable uses*** of the FL ICAN.

(1) Spamming, profanity, sexual content, gaming, etc.

(2) Using the Internet for pornography, access to pornography, or obscene web sites.

(3) Viewing non work related streaming video, advertising or selling personal property, listening to radio broadcasts.

(4) Copyright infringement (such as sharing of copyright material by means of peer–to-peer (P2P) software or loading unauthorized services).

(5) Using e-mail for unauthorized mass mailing, hoaxes, auto-forwarding of official mail to non-official mail accounts, initiating or forwarding scams and chain letters.

(6) Installing personal (home) e-mail accounts on Government computers.

(7) Subscribing to newsletters or list servers that are not related to official job performance or career development.

(8) Unlawful activities, commercial purposes, or in support of "for profit" activities, personal financial gain, personal use inconsistent with DOD policy, or use that violates other Army policies or public law. This may include, but is not limited to violation of intellectual property, gambling, terrorist activities, and sexual or other forms of harassment.

(Note: Activity in any criteria can lead to disciplinary action, suspension or criminal charges)
I understand that DOD policy states that Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems), when use of such systems and equipment is paid for by the Federal Government, will be for "official use" and "authorized purposes" only. AR 25-1 permits some authorized personal uses of Army ISs provided they do not adversely affect the performance of official duties by the employee or employee's organization and they are of reasonable duration and frequency. Whenever possible, these activities should be conducted during personal time, such as during lunch, breaks, and other off-duty periods. Some examples of authorized personal uses are: checking in with spouse or minor children; scheduling doctor, auto, or home repair appointments; and brief internet searches or e-mailing directions to visiting relatives.

I understand that violations of identified policy may result in counseling by supervisor to denial of email and networking services.

7. Common Access Card (CAC)/Public Key Infrastructure (PKI). PKI provides a secure computing environment utilizing encryption algorithms (public/private keys). The CAC is the primary access control mechanism for all Army users (with very few exceptions) to IT resources. I will memorize the PIN and not write it down. I will not share my CAC PIN with anyone. I will not leave the CAC unattended at the workstation.

8. Data at Rest (DAR). DAR refers to the protection of sensitive information and personally identifiable information (PII) stored on computers (workstations, laptops, tablets, etc.), portable hard drives, thumb drives, DVD/CDs, floppy diskettes, and similar storage devices. It excludes data that is traversing a

network, located on the Fort Lee virtual server (VS), or temporarily residing in computer memory to be read or updated. Sensitive information is defined as unclassified Army information not specifically created for public release or access; this includes but is not limited to contract sensitive data, preliminary budget calculations, specifications for new equipment, personnel stationing information, emergency plans or orders, or items that are marked as "For Official Use Only" (FOUO). Personally identifiable information (PII) is defined as sensitive information that can be used to distinguish or trace an individual's identity, such as, but not limited to; name, birth date, home address, social security number, pay information, family information, etc.; this includes but is not limited to personnel action forms (SF-50s), security clearance forms, evaluation reports, recall rosters, or similar documents with similar types of information.

a. I will identify sensitive information and/or PII on IS (including removable media) and ensure it is encrypted with an Army-approved DAR product. Storage of PII on all government computers is generally prohibited.

b. I will not carry sensitive information and/or PII on a mobile IS (including removable media) unless it is absolutely required for my job and authorized by my supervisor. In the event where it becomes necessary to transport PII data on a laptop computer, this data must be encrypted using PoinSec or Microsoft Encrypting File System (EFS).

c. ITO will assist in the installation of the software on laptop computers.

9. Mobile computing devices and removable storage media (USB/thumb drives, CDs, DVDs, diskettes, etc.). Removable media like floppies, CDs, and thumb drives are too easy to lose, misplace, and steal; and they are easily taken off-site. All users must mitigate the risk of compromising information stored on mobile computing devices and removable media. These media have multiple uses and their small size and adaptability can result in loss of accountability and inappropriate cross net use (i.e., NIPRNET to SIPRNET).

a. I will ensure the laptop is labeled to indicate that all sensitive information is protected by an approved DAR solution, and the laptop is authorized for travel.

b. I will ensure removable storage media (RSM) is identified, labeled and accounted for to indicate it is authorized to be off the installation.

c. I will ensure mobile computing devices are hand-carried or under visual observation while traveling on public transportation.

d. I will not leave a mobile computing device overnight in an unattended vehicle, unattended in an unsecure personal residence, or unattended and unsecured in the workplace. Unless in (In addition to being in) a locked office, mobile computing devices should be locked in a container or secured with a cable lock in (to) an immovable object.

10. Wireless systems. Wireless systems provide cost effective solutions for extending wired networks to remote areas. However, it provides an easy means of exploitation. Wireless networks must be secured with encryption. There is no exception to this rule.

a. I will not install wireless access points (stand alone or connected to Army network) without prior approval from the Directorate of Information Management. At no time will any access point be installed in offices as an extension to connect additional computers or printers.

b. Periodic “war driving” scans for wireless network on the installation will be performed by the DOIM. Unauthorized wireless systems will be shut down and equipment confiscated.

11. Failure to agree with the Acceptable Use Policy could result in denial of access to Fort Lee information systems.

1**2. Acknowledgement**. I have read, understand, and have received a copy of the Fort Lee ICAN Acceptable Use Policy (Students), dated 13 July 2010. I understand the requirements regarding use of and access to the FL ICAN. I understand my responsibilities regarding these systems and the information contained in them acknowledges that I may be subject to administrative sanctions or actions under the UCMJ or Federal law for violation of security policy and or procedures.

_____ _____
Last Name, First Name, MI Phone

_____ _____
Signature Date

_____ _____
Course Class Dates

ADDENDUM ITEMS

Items 13 and 14 require individual signature and date of the user. These items are applicable to those individuals using such services/devices/access.

13. "Road Warrior" Laptop Security. Users of mobile computing devices (laptops, portable notebooks, tablet-PCs, and similar systems) are tasked with the physical security of these mobile devices while administrators must protect the IS from compromise when used as a standalone system or when remotely connected. I have read and understand the BBP, "Road Warrior" Laptop Security (found on the https://informationassurance.us.army.mil website.

_____(Signature/Date)

14. Telework Policy. DOD policy states that:

a. No classified documents (hard copy or electronic) may be taken by students to alternative work sites.

b. Government-furnished computer equipment, software and communications, with appropriate security measures, are required for any regular and recurring telework arrangement that involves sensitive unclassified data, including Privacy Act data or For Official Use Only data.

c. Government-furnished equipment must only be used for official duties and family members and friends of students are not authorized to use any Government-furnished equipment. The student must return all Government-furnished equipment and materials to the agency at the conclusion of the course at the activity's request.

d. Students are responsible for the security of all official information, protection of any Government-furnished equipment and property, and carrying out the mission of DOD at the alternative work site.

_____(Signature/Date)