ACCEPTABLE USE POLICY (AUP)

Reference: AR 25-2 (Information Assurance). A well-protected DoD/Army network enables organizations to easily handle the increasing dependence on the Internet. For a DoD/Army organization to be successful, it needs to integrate information that is secure from all aspects of the organization. The purpose of this policy is to outline the acceptable use of computer equipment within a DoD/Army/ARNG organization. These rules are in place to protect the employee and the organization. Inappropriate use exposes DoD/Army/ARNG units to risks including attacks, compromise of network systems and services, and legal issues. This policy applies to all employees, contractors, consultants, temporary employees, and other workers assigned to DoD/Army/ARNG organizations.

By signing this document, I acknowledge I have read the content and will comply.

Last Name | First Name | MI | Area Code and Phone Number

Date | Signature

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained in the Secret Internet Protocol Router Network (SIPRNET) and/or Non-secure Internet Protocol Router Network (NIPRNET) from unauthorized or inadvertent modification, disclosure, destruction, denial or service, and use.

2. Access. Access to this network is for official use and authorized purposes as set forth in DOD Directives 5500.7-R (Joint Ethics Regulation) AR 25-2 (Information Assurance), and ARNG and Army network policy and accreditation.

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

4. Classified information processing. SIPRNET is the primary classified Information System (IS) for Army units. SIPRNET is a classified only system and approved to process SECRET collateral information as SECRET and with SECRET handling instructions.

a. The SIPRNET provides classified communication to external DoD agencies and other U.S. Government agencies via electronic mail.

b. The SIPRNET is authorized for SECRET level processing in accordance with accredited SIPRNET ATO.

c. The classification boundary between SIPRNET and NIPRNET requires vigilance and attention by all users.

d. The ultimate responsibility for ensuring the protection of information lies with the user. 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.

5. Unclassified information processing. NIPRNET is the primary unclassified information system for Army units. NIPRNET is an unclassified system.

a. NIPRNET provides unclassified communication to external DOD and other United States Government organizations. Primarily, this is done via electronic mail and Internet networking protocols such as Web Access, Virtual Private Network, and Terminal Server Access Controller System (TSACS).

b. NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2, the ARNG IA SOP, and local automated information system security management policies. A DAA has accredited this network for processing this type of information.

c. The NIPRNET and the Internet, for the purpose of the AUP, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet, as well as all inbound/outbound data, external threats (e.g. worms, denial of service, hacker) and internal threats.

d. Public Key Infrastructure (PKI) Use:

(1) Public Key Infrastructure provides a secure computing environment utilizing encryption algorithms (Public/Private-Keys).

(2) Token/Smart Card (or CAC). The Cryptographic Common Access Card Logon (CCL) is now the primary access control mechanism for all Army users (with very few exceptions). This is a two phase authentication process. First, CAC is inserted in to a middleware (reader), and then a unique user PIN number provides the validation process.

(3) Digital Certificates (Private/Public Key). CAC is used as a means to sending digitally signed e-mail and encrypted e-mail.

(4) Private Key (digital signature), as a general rule, should be used whenever e-mail is considered "Official Business" and contains sensitive information (such as operational requirements). The digital signature provides assurances that the integrity of the message has remained intact in transit, and provides for the non-repudiation of the message that the sender cannot later deny having originated the e-mail.

(5) Public Key is used to encrypt information and verify the origin of the sender of an email. Encrypted mail should be the exception, and not the rule. It should only be used to send sensitive information, information protected by the Privacy Act of 1974, and Information protected under the Health Insurance Portability and Accountability Act (HIPPA).

(6) Secure Socket Layer (SSL) technology should be used to secure a web based transaction. DoD/Army Private (Intranet) web servers should be protected by using this technology IAW DoD/Army PKI implementation guidance.

6. User Minimum-security rules and requirements. As a SIPRNET and/or NIPRNET system user, the following minimum security rules and requirement apply:

a. I understand personnel are not permitted access to SIPRNET or NIPRNET unless in complete compliance with the DOD, Army personnel security requirement for operating in a SECRET system-high environment.

b. I have completed the required security awareness-training (e.g. Annual AT Awareness Training Level I or Computer Security for Users and provided proof of completion to my IASO. IAW AR 25-2, prior to receiving network/system access, I will participate in all DoD/Army/ARNG sponsored Security Awareness Training and Certification program (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering). I understand that my initial training will expire in one year and that I will be required to take an annual refresher training (IAW AR 25-2) and my account will be disabled until I have met this requirement.

c. I will maintain an Army Knowledge Online (AKO) account (www.us.army.mil) (military network only).

d. I will protect my logon credentials (passwords or pass-phrases). Passwords will consist of at least 14 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs or dictionary words as passwords or pass-phrases.). I will not store my password on any processor, microcomputer, PDA, PED, or on any magnetic or electronic media. Passwords will be changed every 60 days in accordance with DoD/DA/ARNG Security policies.

e. When I use my CAC to logon to the network, I will make sure it is removed prior to leaving the computer that I logged on.

f. I will use only authorized hardware and software on the DoD/Army networks to include wireless technology. I will not install or use any personally owned hardware, software, shareware, or public domain software.

g. 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.

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

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

j. 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.

k. 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.

l. I will not utilize ARNG/Army/DOD provided ISs for commercial financial gain or illegal activities.

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

n. I will use screen locks and log off the workstation when departing the area.

o. 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.

p. I will address any questions regarding policy, responsibilities, and duties to my IASO and/or J6 SA.

q. I understand that each IS is the property of the Army/ARNG and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realized that I should not store data on the IS that I do not want others to see.

r. I understand that monitoring of SIPRNET and NIPRNET 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 an Army 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) Unacceptable use of e-mail include exploiting list servers or similar group broadcast systems for purposes beyond intended scope to widely distribute unsolicited e-mail (SPAM); sending the same e-mail message repeatedly to interfere with recipient's use of e-mail; sending or broadcasting, e-mail messages of quotations, jokes, etc., to multiple addressees; sending or broadcasting unsubstantiated virus warnings from sources other than IAMs (e.g. mass mailing, hoaxes, and auto-forwarding).

(5) 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).

(6) To show what is deemed proprietary or not releasable (e.g. Use of keywords, phrases or data identification).

(7) My local IASO has informed me of TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met.

(8) I will not move hardware or alter communications connections without first getting approval from the SA or IASO (if applicable).

(9) I will scan all magnetic media (e.g., disks, CDs, tapes) for malicious software (e.g., viruses and worms) before using it on a GC, IT system, or network.

(10) I will not transfer information using magnetic media from a classified system to an unclassified system.

(11) I will not forward chain email or virus warnings. I will report chain email and Virus warnings to my IASO and delete the message.

(12) I will not run "sniffers" (utilities used to monitor network traffic, commonly used to Spy on other network users and attempt to collect their passwords) or any hacker- related software on my GC, Government IT system, or network.

(13) I will not download file-sharing software (including MP3 music and video files), peer-to peer software (i.e. Kazaa, Napster) or games onto my GC, Government IT system, or network.

(14) I will not connect any personal IT equipment (e.g., PEDs and PDAs (such as Palm Pilots), personal computers, and digitally enabled devices to my GC or to any Government network without the written approval of my DOIM, IAM, IASO, or information Management Officer (IMO).

(15) I will not use Internet "chat' services (e.g., America Online, Microsoft Network (MSN) Instant Messenger, Yahoo) from my GC. If chat service is needed, I will use my Army Knowledge Online (AKO) account Chat capability or unless approved by the DOIM.

s. I understand that I may use an Army IS for limited personal communications by e-mail and brief internet searches provided they are before or after duty hours, break periods, or lunch time or IAW local policies and regulations, as long as they do not cause an adverse impact on my official duties; are of reasonable duration, and causes no adverse reflection on DOD. Unacceptable use of services or policy violations may be a basis for disciplinary actions and denial of services for any user.

t. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to DoD/Army information systems.

u. I understand that repetitive violation of this AUP, AR 25-2, and/or the ARNG IA SOP security measures will result in the loss of my privilege. I further understand that I will receive a written counseling statement from my first line supervisor, and in order to lift this restriction a memorandum from my Commander/Director (or designated representative) will be required. This request will be routed via the IASO to the installation Information Assurance Manager (IAM). (AKO) account Chat capability or unless approved by the DOIM.

9. 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) I understand that I must undergo a favorable review of local personnel records check, and an initiation of a NACIC (for civilians), or a National Agency Check (NAC) (for military and contractors) Background Investigation, with favorable results or have a current security clearance prior to obtaining and maintain network access (as directed in AR 25-2, Section V). I further understand that if I refuse to submit to a NAC, or if I have a negative result from the NAC, I will be denied network access. I understand that all network access is a revocable privilege.

(2) If I am requesting access to classified systems I understand that I will be required to obtain a Security Clearance at least commensurate with the level of access I require to perform my official duties, and that I must execute a Non-Disclosure Statement, and have favorable security status BEFORE being granted such access.

(3) 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.

(4) At any time, the U.S. Government may inspect and seize data stored on this information system.

(5) 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.

(6) 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.

(7) 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. 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.

(b) 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.

(c) 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 users' 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.

(d) 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.

(e) 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.

(f) 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.

(g) 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 the user of the 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.