SOUTH ATLANTIC REGION INSTALLATION CAMPUS AREA NETWORK (ICAN)
ACCEPTABLE USE POLICY (AUP)

For use of this form, see AR 25-2, Army Best Business Practice 06-PR-M-0003, IA Control ECWM

SECTION I - ACCEPTABLE USE POLICY

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 Fort Eustis, Fort Story and Fort Lee, Virginia. These rules are in place to protect the employee and the organization. Inappropriate use exposes DoD/Army 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 Fort Eustis, Fort Story and Fort Lee Virginia.

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 use, modification, disclosure, destruction, and denial of 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 (JER), AR 25-2 (Information Assurance) and Army network policy and accreditation.

3. Revocability. Access to Army 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 an accredited SIPRNET Approval to Operate (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.

e. Writing to removable media such as USB and DVD/CD drives is prohibited on SIPRNET without express authorization from the AO. Read only privileges are not impacted and are allowed for DoD personnel based on existing procedures, need-to-know and mission need.

5. Unclassified information processing. The NIPRNET is the primary unclassified information system for Army units. 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 a Web Access and Virtual Private Network (VPN).

a. NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2 and local automated information system security management policies. A Authorizing Official (AO) has accredited this network for processing this type of information.

b. 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.

c. 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, the CAC is inserted into a middleware (reader), and then a unique user PIN number provides the validation process.

(3). Digital Certificates (Public/Private-Key). CAC is used as a means for 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 the information and verify the origin of the sender of an e-mail. 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 requirements apply:

a. I understand personnel are not permitted access to SIPRNET or NIPRNET unless they have met the appropriate DoD and Army personnel security requirements for accessing the system.

b. I have completed the required security awareness training (Annual AT Awareness Training Level I or Computer Security for Users) and provided proof of completion to my ISSO. IAW AR 25-2, prior to receiving network/system access, I will participate in all DoD/Army sponsored Security Awareness Training and Certification programs 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 certificate will expire one year from the date that I successfully complete training and that I will be required to complete annual refresher training (IAW AR 25-2). I understand that my account will be disabled if I do not complete the annual certification training by the anniversary date.

c. I will protect my logon credentials (passwords or pass-phrases). Passwords will consist of at least 14 characters with two (2) each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of my 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. IAW AR 25-2, Chapter 4, Section IV, Para 4-12, passwords should be changed at least every 90 days to 150 days.

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/Army networks 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 DoD or Army 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 System Support Officer (ISSO) and cease all activities on the system.

n. I will address any questions regarding policy, responsibilities, and duties to my ISSO and/or the Network Enterprise Center (NEC) Information System Security Manager (ISSM).

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

p. 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 includes 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 or quotations, jokes, etc., to multiple addressees; and sending or broadcasting unsubstantiated virus warnings (e.g. mass mailing, hoaxes, auto-forwarding) from sources to anyone other than the ISSM.

(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). Unauthorized sharing of information that is deemed proprietary or not releasable (e.g. use of keywords, phrases or data identification).

q. 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 cause no adverse reflection on DoD. Unacceptable use of services or policy violations may be basis for disciplinary actions and denial of services for any users.

r. I understand that AR 25-2 is the implementation of Federal Law and is punitive in nature. Violations of paragraphs 3-2, 3-3, 4-5, 4-6, 4-7, 4-10, 4-11, 4-12, 4-13, 4-16, 4-17, 4-18, 4-20, 4-21, 4-22, 4-23, 4-25, 4-30, 6-1, 6-2, and 6-5 of this regulation may be punishable as violations of a lawful general order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or contractual actions as applicable. Personnel are not subject to UCMJ who fail to comply with these requirements may be subject to disciplinary, administrative, or prosecutorial actions.

s. I understand that I will not write to removable media on SIPRNET, such as USB or DVD/CD drives unless specifically authorized, in writing to do so by 7SC AO.

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

a. I am 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. I 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, 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 system includes security measures (e.g., authentication and access controls to protect U.S. Government interests; not for my 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 counter-intelligence 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 part 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 standard and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an IS, 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 no 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.

c. 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.

d. 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. 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 provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

e. In the event of this User Agreement being revised or updated, I will read and re-sign the most recent version.

Directorate/Division/Branch	**Phone Number with Area Code**
Last Name, First, MI (print)	**Rank/Grade**

Digital Signature/Date:

SECTION II - ADDENDUM ITEMS
Items 8, 9, 10, 11, 12, 13 & 14 require an ADDITIONAL SIGNATURE on page 6

8. Remote Access.

a. Remote access will be via Virtual Private Network (VPN), or Outlook Web Access (OWA). Government owned hardward and software will be used. The employee is the only individual authorized to use this equipment. Access will be as authorized by the supervisor. Requirements as indicated throughout this AUP are applicable for access to the USG resources.

b. I have completed required training at https://iatraining.us.army.mil and I acknowledge the following:

(a). I understand that I must always maintain physical control of my authorized device.

(b). I understand that I must take necessary precautions to reduce the exposure of sensitive data.

(c). I understand that I am responsible backing up own data frequently.

(d). I understand the requirements for user authentication, anti-virus software, the use of a personal firewall when required, and the requirement to encrypt PII, sensitive, and operational data.

(e). I understand that I am only to enable wireless interfaces when needed.

(f). I understand the requirement to enable a VPN connection to the DoD network immediately after establishing a wireless connection.

(g). I understand that all Internet browsing will be done via a VPN connection to the DoD network.

(h). I understand that there will be no split tunneling of VPN.

(i). I understand the locations where wireless remote access is authorized or not authorized (i.e., home, airport, hotel, etc.).

(j). I understand the wireless client configuration requirements.

(k). I understand that I am required to use WPA2 Personal (AES) on my home WLAN.

(l). I understand the Home WLAN password and SSID requirements and I am to discontinue the use of devices suspected of being tampered with and notify my site IAO.

(m). I understand that for iOS devices I must select the “Forget the Network” while still in physical range. (This will prevent the device from automatically joining a network later that may share the same SSID. I understand that I will not be able to “forget” individual networks when out of range and will need to reset all network settings.)

9. "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 at http://doim-knowledge.eustis.army.mil/twiki/pub/InformationAssurance/AcceptableUsePolicy/BBP_Road_Warrior_VER_1_3.pdf).

10. Blackberry Devices

a. I will be held responsible for damage caused to a Government system or data through negligence or a willful act.

b. I am not authorized and will not use Bluetooth technology with Blackberry devices except for the authorized CAC sled found on the Army-approved two way wireless email device listing.

c. I will not operate a wireless device in areas where classified information is electronically stored or processed.

d. I will ensure the Blackberry handheld device is cradled or synced at least once every 30 days to the Blackberry Enterprise server (BES) to receive updated keys and/or software updates.

e. I understand that all charges incurred in excess of the normal monthly service charge will be the responsibility of the Blackberry user. Charges will be incurred for the following misuses of the device: exceeding allocated minutes per month, use of text messaging, downloading of any services, ring tones, games, etc.; neglect or abusive damage to the device or accessory.

f. I understand that should my Blackberry device be involved in an Unauthorized Disclosure of Classified Information (UDCI) on the NIPRNET, the device will be wiped and secured by my organization (ISSO/ISSM) and that it will not be allowed to be used ont he NIPRNET again.

g. I have completed DoD wireless training at http://iase.disa.mil/eta/pedrm_v2/pedrm_v2/launchPage.htm and local wireless training at https://airborne.bragg.army.mil/NEC_BB_Trg/. I have provided my certificates to my IMO and have ensured my training is updated in my ATCTS profile. As a part of completing my required wireless training I acknowledge the following:

(a). I understand that personally-owned PEDs will not be used to transmit, receive, store, or process DoD information unless approved by the DAA and I sign a forfeiture agreement in the case of a security incident.

(b). I understand the procedures for using wireless devices in and around classified processing areas.

(c). I understand the requirement that PEDs with digital cameras (still and video) are not allowed in any SCIF or other areas where classified documents or information is stored, transmitted, or processed.

(d). I understand the requirement that wireless email devices and systems are not used to send, receive, store, or process classified messages. (Exception: SME PED)

(e). I understand that smartphone devices and systems will not be connected to classified DoD networks or information systems.

(f). I understand that I must immediately notify appropriate site contacts (i.e., IAO, smartphone management server administrator, supervisor, etc.) when if my smartphone has been lost or stolen.

(g). I understand the additional requirements for Secure Bluetooth Smart Card Reader (SCR) usage if I have been authorized:
--Secure pairing procedures.
--Perform secure pairing immediately after the SCR is reset.
--Accept only Bluetooth connection requests from devices they control.
--Monitor Bluetooth connection requests and activity in order to detect possible attacks and unauthorized activity.

(h). I understand how to sign and encrypt email.

(i). I understand that if authorized the use of the Short Message Service (SMS) and/or Multi-media Messaging Service (MMS) are used there are additional SMS/MMS security issues.

(j). I understand that Over-The-Air (OTA) wireless software updates should only come from DoD sources. Software updates from the wireless carrier or other non-DoD sources will not be used until the download has been tested and approved by the IAO.

(k). If authorized the use of the carrier's Wi-Fi Service the I understand the following:
--Procedures for setting up a secure Wi-Fi connection and verifying that the active connection is to a known access point.
--Approved connection options (i.e., enterprise, home, etc.).
--Requirements for home Wi-Fi connections.
--The Wi-Fi radio must never be enabled while the smartphone is connected to a PC.

(l). I understand that I am not to discuss sensitive or classified information on non-secure (devices not FIPS 140-2 certified or NSA Type-1 certified for voice) cellular phones, cordless phones, and two-way radios used for voice communications.

(m). I understand that I am not to connect PDAs and smartphones to any workstation that stores, processes, or transmits classified data. (Exception: SME PED)

(o). I understand that I must manually download updates to antivirus and personal firewall application at least every 14 days if automatic updating is not available. (Applies only if my specific PDA / smartphone device has an antivirus / personal firewall application(s).

11. Short Messaging Service (SMS) on Blackberry/Wireless Devices

I am aware of the following risks when utilizing the SMS service:

a. Messages are not encrypted and copies are stored in memory on the phone and in the wireless carrier database. Sensitive information will not be sent via SMS/Text/Messages/Multimedia Messaging Service (MMS).

b. URL to hacker websites can be sent to a SMS/Text Message/MMS. If a user connects to the URL, malware could be downloaded on the phone.

c. Executable files (including malware) can be embedded in SMS/Text Message/MMS.

d. Photos sent via SMS/Text Messages/MMS can have URLs to hacker websites embedded in the photo. When the photo is viewed the phone will connect to the website of the embedded website.

e. Photos sent via SMS/Text Messages/MMS can have the executable files (including malware) embedded in the photo. When the photo is viewed the phone will execute the file.

12. Data at Rest

OPORD 0910-300, 9th SC (A) has tasked all subordinate Commands with the requirements to implement one of three Data at Rest (DAR) encryption solutions, which are Microsoft BitLocker, Mobile Armor or Microsoft Encrypting File System (EFS). This includes all Mobile computing devices (e.g. laptops, PDAs and Blackberry devices), and all desktop systems with the enabled capability to write to CDs or host USB mobile storage devices. Unlike BitLocker or Mobile Armor, EFS requires affirmative action on behalf of the end user to ensure important data is encrypted and properly stored. All sensitive information must be stored in the encrypted file directory to be properly protected. Individuals who do not take the proper steps to protect sensitive data are subject to administrative, disciplinary, and/or criminal penalties. If I am using EFS I understand that I have the following responsibilities:

a. Ensure all compliance with this DAR Policy when using Mobile Computing Devices (MCDs).

b. Ensure files and folders that contain sensitive information are placed into the EFS folder when stored on any form of media to include MDCs and Desktops.

c. Ensure the "My Documents" folder is not encrypted.

d. Ensure domain login based encryption recover keys (password or non-password protected) are not stored on desktops or MCDs that are used to process or store sensitive information.

e. Ensure encrypted files are not forwarded, saved, or copied to a network share or MCD that is not formatted for NTFS, as it will result in a loss of encryption.

f. When transporting files to another device, ensure the encryption key is imported to the designated desktop or MCD prior to transporting encrypted files. Once a file is encrypted, the user will not be able to access the NTFS files from another device unless the encryption key is imported to the device.

Should you not feel confident that you understand how to properly use EFS, it is your responsibility to contact your local ISSM/ISSO for further guidance.

13. Writing to Removable Media on SIPRNET

IAW CTO 10-133, Writing to removable media on SIPRNET is prohibited unless authorized and approved.

I understand that I have the following responsibilities:

a. If authorized and approved to utilize 'write' capabilities on SIPRNET, I understand that I must utilize the two person integrity (TPI) rule.

b. I must keep a log of each and every data transfer and ensure all required log items are completed, and that the second person under the TPI rule will witness each and every data transfer and complete the log as a witness.

c. I understand that AR 25-2 is the implementation of Federal Law and is punitive in nature. Violations of paragraphs 3-3, 4-5, 4-6, 4-12, 4-13, 4-16, 4-20, and 6-5 of this regulation may be punishable as violations of a lawful general order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or contractual actions as applicable. Personnel who are not subject to UCMJ who fail to comply with these requirements may be subject to disciplinary, administrative, or prosecutorial actions.

14. Social Media Usage Agreement

The Department of Defense does not necessarily endorse, support, sanction, encourage, verify or agree with the comments, opinions, or statements posted on any social media website. Any information or material placed online, including advice and opinions, are the views and responsibility of those making the comments and do not necessarily represent the views of the Department of Defense, the United States Government or its third party service providers. By submitting a comment for posting, you agree that the Department of Defense, the United States Government and its third party service providers are not responsible, and shall have no liability to you, with respect to any information or materials posted by others, including defamatory, offensive or illicit material, even material that violates this Agreement. For more information or to download the U.S. Army Social Media Handbook, go to https://www.army.mil/media/socialmedia/

a. I understand that everything written or posted on social media sites is public and may remain permanently in the public domain, even if I attempt to delete it.

b. I will take personal responsibility for my posts -- including comments, photos, blogs and documents.

c. I will utilize the security settings provided by social media sites to ensure my accounts are configured properly to restrict the public from accessing my personal data. I will also safeguard my passwords and the answers to my personal security questions.

d. I will not conduct official government business through my personal email account, file-sharing websites, or social media websites.

e. When posting to any website from **ANY hardware or network**, I will avoid mentioning:

(1). DoD unit locations. This includes posting photos that include geographical location data (also known as "geotagging"), which may provide key location information of deployed DoD unit(s). This also includes current and future locations of military units and ships, descriptions of overseas bases, or discussions of areas frequented by service members overseas.

(2). Troop movement dates/times -- information regarding times and dates of future formations that could be used to coordinate attacks on military members. This includes drill schedules, training schedules and dates of upcoming exercises and deployments.

(3). Technical equipment specifications/capabilities and/or details of weapons systems.

(4). Daily military activities and operations, unit morale, and results of operations.

f. **While using DoD hardware or networks**, I will refrain from posting comments or photos that:

(1). contain threats, obscenity, material that would violate the law if published, abusive, defamatory or sexually explicit material.

(2). contain obscene or threatening language or discrimination (hate speech) based on race, sex, gender, religion, national origin, age, or disability.

(3). suggest or encourage illegal activity.

(4). attempt to defame or defraud any financial, commercial, governmental or non-governmental agency.

(5). contain credit card numbers, social security numbers, street addresses, personal phone numbers or other sensitive PII (personally identifiable information)

(6). contain my password(s) or answers to my security questions. I will protect my logon credentials (passwords and/or pass-phrases).

(7). contain material protected by copyright or trademark without express permission from the owner.

(8). contain derogatory comments expressed against the chain of command.

(9). contain the use of my rank, job and/or responsibilities in order to promote myself for **personal or financial gain**.

Digital Signature/Date: