SPS-A Rules of Behavior

a. I understand that I have no expectation of privacy with respect to any information, either official or personal, transmitted over, or stored within any Army IS to include information stored locally on the hard drive or other media including removable media or hand-held peripheral devices.

b. I understand that personnel are not permitted access to the A-WAN unless in complete compliance with the DoD and ALTESS personnel security requirements for operating in a SBU system-high environment.

c. I will generate, store and protect passwords, pins and pass-phases for the IS I am accessing. Passwords will be in keeping with AR 25-2 with a minimum of fifteen (15) characters and will include a minimum of two each uppercase letters, lowercase letters, numbers and special characters. I am the only authorized user of this account. I will not store my passwords on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or on any magnetic or electronic media. I will not use my user id, common names, birthdays, phone numbers, military acronyms, call signs or dictionary words as passwords or pass-phrases.

d. I understand that commercial electronic mail (e-mail) accounts are prohibited for work-related communication.

e. When sending e-mail, I will identify myself as a contractor within my e-mail signature, and I will use a standard signature block (if applicable).

f. I will not use Internet "chat" services including, but not limited to, America Online, Google, Microsoft Outlook express or Yahoo Instant Messenger on my Government Computer. If chat services are required, I will use my Microsoft Teams account.

g. When in an official or personal capacity, I will use electronic communications that is consistent with Army Values and Standards of Conduct. I will "Think, Type, Post." I will "Think" about the message being communicated and who could potentially view it, "Type" a communication that is consistent with Army Values, and "Post" only those messages that demonstrate dignity and respect for self and others.

h. When on social media platforms, I will not comment, post, or provide links to material that violates the UCMJ or the basic rules of the Soldier's conduct.

i. I will not use electronic communication (signs, writing, images, sounds, or data) transmitted by computer, phone, or other electronic device to inflict harm. Examples include, but are not limited to: harassment, bullying, hazing, stalking, discrimination, retaliation, or any other types of misconduct that undermine dignity and respect. Electronic communication include, but are not limited to: text messages, emails, chats, instant messaging, screensavers, blogs, social media sites, electronic device applications, and web/video conferencing.

j. I will use virus-checking procedures before uploading or accessing information from any system, e-mail attachment or removable media and insure virus definition files are no older than one week.

k. I will not attempt to access or process data exceeding the authorized Information System (IS) classification level, now will I transfer information from a classified IS to an unclassified IS.

l. 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.

m. 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.

n. I will never leave my IS unattended while I am logged on unless the IS is protected by CAC removal or other screen-locking protection.

o. I will immediately report any suspicious output, files, shortcuts or system problems to my designated Point of Contact (POC) and cease all activities on the system. Additionally, if I observe anything on the system I am using that indicates inadequate security, I will immediately notify my POC.

p. I will not connect any government or privately owned hardware such as PEDs, PDAs, personal computers, laptops, memory sticks (a.k.a. thumb drives), MP3 players, or mass storage devices to the Government IS. I understand that any use of personally owned hardware is prohibited without the expressed written consent of the Information Assurance Manager (IAM).

q. I will address any questions regarding policy, responsibilities and duties to my POC, and I will comply with all security guidance issued by my POC.

r. While at the ALTESS facility, I will not enter areas labeled as a "Restricted Area" unless I have a need and authorization to do so. Additionally, I will be aware of the TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections without first getting approval from the ALTESS IAM.

s. I understand that each IS is the property of the Army 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 realize that I should not store data on the IS that I do not want others to see.

t. I understand that monitoring of the A-WAN will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or criminal prosecution. I understand that the following activities define unacceptable uses of an Army IS:

    1. Use ISs for personal commercial gain or illegal activity (e.g., Ebay activity or the sharing of copyrighted material).
    2. I will not forward chain e-mail or virus warnings. I will report chain e-mail and virus warnings to my POC.
    3. Use ISs in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army or violates standards of ethical conduct.
    4. Accessing, storing, processing, displaying, distributing, transmitting and viewing material that is; pornographic, threatening, harassing, political, racist, defamatory, vulgar, hate-crime related, subversive in nature, or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, national, or international law.
    5. Participate in on-line gambling or other activities inconsistent with public service.
    6. Participate in, install, configure or use the IS in any commercial or personal distributed computing environment (DCE).
    7. Attempt to strain, test, circumvent, bypass security mechanisms or perform network or keystroke monitoring, nor attempt to mask or hide my identity, or to try to assume the identity of someone else. I will not run "sniffer" or any hacker-related software on my IS.
    8. Modify the system equipment or software, use it in any manner other than its intended purpose, introduce malicious software or code or add user-configurable or unauthorized software (e.g., instant messaging, peer-to-peer applications).
    9. Relocate or change IS equipment or network connectivity of IS equipment without proper security authorization.
    10. Disable or remove security or protective software or mechanisms and their associated logs.
    11. Use of Universal Serial Bus (USB).

u. In the event of data spillage, I will immediately 1) Contact the AESD via telephone to report the incident (DO NOT SUBMIT CLASSIFIED DATA TO THE AESD), 2) Log out of the SPS-A system, and 3) Contact my local Security Manager to report the incident.

Acknowledgement. I have read the above requirements regarding use of the SPS-A system. I understand my responsibilities regarding this system and the information contained in it. I affirm that the I have the necessary security awareness training, baseline certification, and computing environment certification (IAW DoD Directive 8570) for the level of access being provided. I understand that I am subject to disciplinary action if I violate DoD computer policy, which may include being subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ).