DEPARTMENT OF THE ARMY
UNITED STATES ARMY ACQUISITION SUPPORT CENTER
9900 BELVOIR ROAD, BUILDING 201, SUITE 101
FORT BELVOIR, VIRGINIA 22060-5567

SFAE-SPA

MAR - 9 2007

MEMORANDUM FOR HEADQUARTERS, UNITED STATES ARMY ACQUISITION SUPPORT CENTER (HQ, USAASC), FORT BELVOIR, VA 22060

SUBJECT: Policy on Acceptable Use of USAASC Network

Effective the date of this memorandum, all HQ, USAASC network users will be required to complete annual security awareness training and sign USAASC's Acceptable Network Use agreement (enclosed).

Authority: DoD 5500.7R, "Joint Ethics Regulation"

Purpose: To implement a signed policy that supports acceptable use of the network and the annual training requirements of USAASC personnel required by DoD 5500.7R.

Special Instructions: Each individual will be required to annually complete user security awareness training and sign a statement of acceptable use of network resources.

This policy is valid until rescinded.

Enclosure

CRAIG A. SPISAK
Director

CF:
PD ALTESS, John W. Tuttle

United States Army Acquisition Support Center
Acceptable Network Use Agreement
Policy

1. **Understanding.** I, the undersigned, understand that I have the primary responsibility to safeguard the information contained in the United States Army Acquisition Support Center (USAASC) Network from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use. I will use Army information systems (computers, systems, and networks) only for authorized purposes.

2. **Access.** Access to the USAASC Network is for official use and 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. **Information processing.** The USAASC Network is the primary unclassified information system for USAASC.

a. The USAASC Network is defined as the USAASC Information System (IS) which contains all of its networked components and includes all Government owned Portable Electronic Devices (PEDs). The PEDs are portable ISs or devices with the capability of wireless or local area network (LAN) connectivity. These include, but are not limited to, cell phones, pagers, personal digital assistants (PDAs) (for example, Palm Pilots, Blackberrys, Pocket PCs), laptops and two-way radios. Current technologies (infrared, radio frequency, voice, video, micro-wave) allow the inclusion of several of these capabilities within a single device and dramatically increase the risks associated with IS and Network access.

b. The USAASC Network 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 http and https.

c. The USAASC Network is approved to process information considered as Sensitive but Unclassified (SBU) and handled and protected as For Official Use Only (FOUO).

d. The USAASC Network and the Internet, as viewed by USAASC, are synonymous. Emails and attachments are vulnerable to interception as they traverse the Non-Classified Internet Protocol Router Network (NIPRNet) and Internet.

5. **Minimum security rules and requirements.** As an USAASC Network system user, the following minimum security rules and requirements apply:

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

b. I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I will generate, store and protect passwords, personal identification numbers and pass-phrases. Passwords will be in accordance with AR 25-2, "Information Assurance," with number of characters, uppercase letters, lowercase letters, numbers and special characters. I am the only authorized user of this account and will not share my password among users. I will not store my password on any processor, microcomputer, PDA, PED, or on any magnetic or electronic media. I will not use my user-ID, common names, birthdays, phone numbers, military acronyms, call signs, slang, consecutive or repetitive characters or dictionary words as passwords or pass-phrases.

d. I will not use any privately owned hardware such as PEDs, PDAs, personal computers, memory sticks (a.k.a. thumb drives), MP3 players, or mass storage devices. I understand any use of personally owned hardware is prohibited without the expressed written consent of the Information Assurance Security Officer (IASO).

- No non-Government laptops, computers, or servers will be attached to the USAASC network.

e. I will not install or use any personally owned software, shareware or public domain software. I will not download file-sharing software (including music and videos files). I understand that:

- All software must be approved and installed by USAASC-Helpdesk.
- A software license is required for each machine with loaded software.
- The USAASC-Helpdesk will keep and maintain original software disks.

f. I will not use Internet "chat" services (e.g., America Online, Google, Microsoft Outlook express or Yahoo Instant Messenger) on my Government Computer. If chat services are required, I will use my Army Knowledge On-Line (AKO) account.

g. I will use virus-checking procedures before uploading or accessing information from any system, e-mail attachment or removable media.

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

i. I will not alter, change, configure or use operating systems or programs, 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. I understand that classified processing/storage is not authorized on any USAASC computer except those designated as SIPRNet.

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

m. I understand that all maintenance will be performed by a Command-designated System Administrator (SA) only.

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 an SA and/or IASO and cease all activities on the system.

- If you suspect you have opened a message, file or program with a virus, disconnect your computer from the network immediately and call the USAASC - Helpdesk (to disconnect from the network remove telephone type cable from the back of your computer). Do not reconnect your computer until someone from the USAASC - Helpdesk has checked your machine.
- All users, to include SAs, will report network security incidents to the USAASC - Helpdesk.
- A few examples of security incidents that must be reported to the USAASC - Helpdesk are: viruses, chain letters, e-mail hoaxes, suspected or actual unauthorized intrusion, unexplained anomalies, possible or actual password compromised, a PC being operated without anti-virus software, and reconfiguration of a PC without permission. Any situation that "does not seem right" should be reported to the USAASC – Helpdesk.
- The point of contact (POC) for Information Security issues is the IASO at commercial (703) 805-1056 or DSN 655-1056.

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

q. 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 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 realize that I should not store data on the IS that I do not want others to see.

r. I understand that monitoring of the USAASC Network 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:

- Using ISs for personal commercial gain or illegal activity (e.g., Ebay type of activity or the sharing of copyright material). This includes use of pornography, or access to pornography web sites, unofficial advertising, soliciting or selling via e-mail, private commercial activities, and other uses that are incompatible with public service.
- Accessing and/or downloading pornographic, sexually explicit, or offensive material.
- Spending excessive time on the Internet, i.e., "surfing the net", resulting in a loss of individual productivity and /or having an adverse impact on mission accomplishment, as determined by an individual's supervisor.
- Forwarding chain e-mail or virus warnings; *Note: report chain e-mail and virus warnings to my IASO.*
- Using ISs in any manner that interferes with official duties that undermine readiness, adversely effects the Army or violates standards of ethical conduct.
- Intentionally send, store, or propagate sexually explicit, threatening, harassing, political or unofficial public activity communications.
- Participating in on-line gambling or other activities inconsistent with public service.
- Recreational use of the World Wide Web (WWW) through Government resources.
- Recreational use of web traffic includes: basketball, golf, and general sports sites, stock market sites, gaming sites, greeting card sites, and multimedia sites.
- Visiting untrusted Internet sites; be certain of the source before downloading and opening files. Seek prior approval to download software from the Internet.
- Control and posting of WWW pages is restricted to designated web-masters.
- Unofficial Audio Streaming. Listening to radio stations via the Internet.

- Unofficial Video Streaming.
- Use of commercial Internet mail (e.g., AOL, MSN, Earthlink, etc.) services is not authorized from an Army network.
- Participating, installing, configuring or using ISs in any commercial or personal distributed computing environment (e.g., human genome research, etc.).
- Releasing, disclosing or altering information without the consent of the data owner, the original classification authority as defined by AR 380-5, "Information Security Program," the individual's supervisory chain of command, the Freedom of Information Act official, the Public Affairs Office or the disclosure officer's approval.
- Attempting to strain, test, circumvent, bypass security mechanisms or perform network or keystroke monitoring; attempting to mask or hide my identity, or try to assume the identity of someone else; running "sniffer" or any hacker-related software on my IS.
- Modifying system equipment or software; using IS in any manner other than its intended purpose; introducing malicious software, code or add user-configurable or unauthorized software (e.g., instant messaging, peer-to-peer applications, or games).
- Relocating or changing IS equipment or network connectivity of IS equipment without proper security authorization.
- Disabling or removing security or protective software mechanisms and their associated logs.

6. **Out processing.** Prior to departing the USAASC, I understand that I must out process through the USAASC- Helpdesk. Any equipment I have signed out will be returned prior to my departure from USAASC. Also, I will remove email forwarding to USAASC from AKO mail settings.

7. **Acknowledgement.** I have read the above requirements regarding use of USAASC access systems. I understand my responsibilities and the information contained in these systems.

Division	Date
Last Name, First, MI	Federal Grade
Signature	Phone Number