ACCEPTABLE USE POLICY
Virtual Army Community Services (VACS) System
Version: 1 DEC 2008

References:
AR 25-2 Information Assurance
AR 380-5 Department of the Army Information Security Program
DoD CIO Memorandum: 09MAY2008, Policy on Use of DoD IS Standard Consent Banner and User Agreement

As a Federal Government employee, Permanent, Temp, or Contractor to the government, and a user of the Virtual Army Community Services (VACS) government automated information systems (AIS), computer equipment and software, you are responsible for understanding and complying with the provisions of AR 25-2, and AR 380-5, and agree to adhere to the security rules noted below. This memorandum is directive in nature but not all-inclusive. Upon signing, you will be provided a copy of this memorandum and the original will be maintained by the Installation Information Assurance Security Officer (IASO or IAM) and is subject to inspection.

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

- 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.
- You consent to the following conditions:
    - 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.
    - At any time, the U.S. Government may inspect and seize data stored on this information system.
    - 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.
    - 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.
    - 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:
        - 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.
- 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.
- 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.
- 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.
- 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.

o 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.

- 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.

Specific responsibilities include:

1. I know I am subject to disciplinary action for any violation or abuse of access privileges per AR 25-2, Chp 1, para 1-1, sub para j.
2. Family and Morale, Welfare and Recreation Command enforces the policy to configure ISs to implement the principle of least user privileges through automated or manual means for access to system resources or information. This means absolutely no Administrator permissions! Exceptions will only be made after IT personnel have physically visited the IS to verify program requires Administrator privileges to run.
3. I know that the use and access to DoD Telecommunication and Information Systems (IS) is a revocable privilege.
4. I acknowledge that the use of official DoD Telecommunication and ISs consent to Information Systems Security Monitoring at all times.
5. I will use ISs only for, and IAW, my official government duties which include access only to that data, control information, software, hardware, and firmware for which I am authorized access and have a need to know, and assume only authorized roles and privileges.
6. I will practice safe network and internet operating principles and take no action that threatens the integrity of the system or network.
7. I acknowledge and understand that certain activities are never authorized on Army networks. These activities are specifically prohibited and per AR 25-2, chp 3, para 3-3, sub para(2), **I will not** –
    a. Use IS's for my personal commercial gain or illegal activities.
    b. Use IS's in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army or violates standards of ethical conduct.
    c. Intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications.
    d. Participate in on-line gambling or other activities inconsistent with public service.
    e. Participate in, install, configure, or use IS's in any commercial or personal Distributed Computing Environment (DCE) (for example, SETI, human genome research, etc).
    f. Release, disclose, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380–5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval.

g. Attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring.
h. 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 (for example, instant messaging, peer-to-peer applications).
i. Relocate or change IS equipment or the network connectivity of IS equipment without proper security authorization.
j. Share personal accounts and passwords or permit the use of remote access capabilities by any individual.
k. Disable or remove security or protective software or mechanisms and their associated logs

8. Furthermore I will not install any software/hardware to any computer or connect any device to the Army network (e.g., a client, or workstation, server, pen drive, or other storage device, printer, switch, hub, or wireless device) without the written prior approval of the Information Assurance Manager (IAM) or the Information Assurance Security Officer (IASO).
9. I will not violate any system accreditation or use any unauthorized software.
10. I will not attempt to access or modify data, crack or change passwords, or use operating systems or programs, except as specifically authorized IAW with my official duties.
11. I will be issued a USERID and password to authenticate logging onto ISs.
    a. I am responsible for all activities that occur under my USERID. I will not permit anyone else access to ISs using my USERID nor will I share my password.
    b. Immediately upon first logon, I will be required to change the individual default password issued to me, to a complex password. Department of the Army and AKO policy defines a complex password as consisting between 14 characters and conforms to the following minimum requirements; passwords must contain a minimum of 2 characters of each of the following: 2 UPPER CASE, 2 lower case, 2 numbers, and 2 special characters.
    c. I understand I will be required to change my password when prompted to do so as directed by Army and/or local policy. I will ensure my password meets current standards (e.g., length, character set, no prohibited sequences, or combinations), as directed by the IAM.
    d. I will not store my password on any processor or microcomputer or on any recordable media unless approved in writing by the IAM.
12. I will never leave my computer unattended and logged-on unless secured by an appropriately password protected screen saver.
13. I know it is a violation of policy for any user to seek to mask or hide his or her identity, or to seek to assume the identity of another.
14. I know the use of employee-owned information systems (EOIS) is prohibited for classified or sensitive information.
15. I know the use of an EOIS for ad-hoc (one-time or infrequent) processing of unclassified information is restricted and only permitted with Information Assurance Manager (IAM) and Designated Approving Authority (DAA) approval.

16. If connected to the Army SECRET Internet Protocol Router (SIPR) Network or SDREN Network, I know:
    a. My system operates at least in the US SECRET, "system-high" mode of operation.
    b. Any recordable media used on the system (pen drive, or other storage device), immediately becomes classified and protected at the system-high level, regardless of the implied classification of any data contained on them (until declassified or downgraded by an approval process and approved by the IAM).
    c. I must protect all printed output at the system-high level until I, or someone with the requisite clearance personally reviews it and classifies (grades) it as to actual content.
    d. I will not enter data into the system if the data is of a higher classification level than the system. I will not enter data that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the IASO.
    e. Only US cleared personnel with a valid need-to-know are allowed access to the system.
    f. Recordable media may not be removed from the computer area without local commander approval.
17. I will check all media for malicious software and scan for viruses before loading on any system.
18. I will not forward or reply to chain e-mail, Spam, or distribute virus warnings. I will report chain e-mail, Spam or virus warnings to my IAM and delete the message. I will not attempt to run sniffer or other hacker-related software on the system.
19. I know what constitutes a security incident. If I observe anything that indicates inadequate security for this system, I must immediately report them to the IAM. I will comply with security guidance issued by my IAM or IASO.
20. I understand there are many more procedures, official regulations and policies applicable to information system operations, and this certificate is only a short summary to stress key points.