SFL-TAP VOW ACCEPTABLE USE POLICY (SFL-TAP VOW AUP)

This computer you are using is owned and monitored by the Department of Defense and the United States Army. It is connected to the computer network known as Soldier for Life-Transition Assistance Program Veterans Opportunity to Work (SFL-TAP VOW).

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 organization. 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 the DoD/Army organizations.

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained within the SFL-TAP VOW network and from unauthorized or inadvertent use, modification, disclosure, destruction, and denial of service.

2. Access. Access to this network access point is for official use and authorized purposes only.

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

4. Writing to removable media such as USB drives, Thumb Drives, Flash Drives and DVD/CD drives is prohibited on any computer/laptop within the SFL-TAP VOW program without express authorization from the IMB (Information Management Branch).

5. Unclassified information processing. The SFL-TAP VOW network is an unclassified information system for Army units and provides unclassified communication to external DoD and other United States Government websites. Primarily, this is done via electronic mail and Internet networking protocols.

6. User Minimum-security rules and requirements. As an SFL-TAP VOW system user, the following minimum-security rules and requirements apply:

a. When I use my CAC to logon to authorized Army websites, I will ensure it is removed and I am logged off prior to leaving the computer.

b. I will not install or use any personally owned hardware (including removable drives, thumb drives, flash drives, USB drives, or DVD / CD ROM), software, shareware, or public domain software.

c. To protect the systems against viruses or spamming, I will use virus-checking procedures before uploading or accessing information from any internet system.

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

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

f. 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.

g. I will address any questions regarding policy, responsibilities, and duties to DHR – IMB personnel only.

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

i. I understand that monitoring of this network access point will be conducted for various purposes and information captured during monitoring may be used for possible adverse administrative, disciplinary or criminal actions.

j. I understand that the following activities are prohibited uses of an Army IS:

1) Unethical use (e.g. Spam, profanity, sexual misconduct, gaming, extortion).

Initial _____

2) Accessing and showing unauthorized sites (e.g. pornography, 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 of 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 IAM.

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).

k. 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 a basis for disciplinary actions and denial of services for any user.

l. 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). These requirements may be subject to disciplinary, administrative, or prosecutorial actions.

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 systems 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:

Initial _____

i. 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.

ii. 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 party and does not negate any applicable privilege or confidentiality that otherwise applies.

iii. 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 IS, if the user intends to rely on the protections of a privilege or confidentiality.

iv. 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.

v. 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.

vi. 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.

_____ _____

Last Name, First, MI Rank/Grade

_____ _____

Signature Date