Womack Army Medical Center (WAMC)
Information System (WIS) Acceptable Use Policy
Sensitive Unclassified Information (SUI) Form
IAW AR 25-2 Dated 10 Mar 2014

Proponent agency for this form is MCXC-IMD

1. References:

a. Army Regulation 25-2, Rapid Action Revision 23 March 2009, Department of the Army Information Assurance Program

b. "Road Warrior" Laptop Security Version 1.0, Dated 17 February 2006

c. Army Regulation 380-5, 29 September 2000, Department of the Army Information Security Program

d. HIPAA, Federal Register, 20 February 2003, Health Insurance Reform: Security Standards

e. DA Memorandum: Security Alert 03-011, Use of Thumb Drive Digital Storage Devices in Sensitive Compartmented Information Facility (SCIF).

f. 03-PE-O-0004, Control of Removable Media, 29 February 2012, IA Best Business Practice

g. Directive-Type Memorandum 09-26, Responsible and Effective Use of Internet based Capabilities, 25 February 2010

2. Understanding. I understand that I have the primary responsibility to safeguard the information used/contained on the unclassified network Womack Army Medical Center's (WAMC) Local Area Network (LAN) from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

3. Access. As a user of the DoD network I understand that…

- I have the primary responsibility to safeguard the information available over the LAN.
- Access to this network(s) is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulations" or as described in this document.
- Access to Army resources is a revocable privilege and is subject to monitoring without notification.
- Ultimate responsibility for ensuring the protection of information lies with the user. The release of Sensitive information through the LAN is a security violation and will be investigated and handled as a security violation or as a criminal offense.
- The LAN 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 web, ftp, secure telnet, SMTP.

- The LAN is approved to process UNCLASSIFIED, SENSITIVE information in accordance with WAMC's local policies.

- The LAN and the internet in this document are synonymous. Electronic correspondence and attachments are subject to interception and monitoring as they traverse the NIPRNET and internet.

- I have completed the Cyber Awareness Challenge training module on the Fort Gordon website. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and nonstandard threats such as social engineering) before receiving system access.

Each Information System (IS) is the property of the Army and is provided for official and authorized use. I further understand that each IS, is subject to monitoring 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. I realize that any data stored on the IS can be accessed by other authorized users.

- Monitoring of the LAN will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.

- I will be required to change my temporarily assigned password IAW published regulations or commander's policy.

- Access to Internet-based capabilities may at any time be temporarily limited on an as-needed basis in order to preserve operations security (OPSEC), to safeguard a mission or to address bandwidth constraints.

- The LAN is certified to process sensitive information. Information classified higher than sensitive is prohibited from being processed.

- The LAN is open to external communications with other facilities in the North Regional Medical Command, the AMEDD, the Army, the DoD, the federal government, and authorized users.

- Primary communication with external entities is via electronic mail and the Internet.

- E-mail and Internet communications are subject to interception; therefore, users must avoid transmitting sensitive information including Electronic Protected Health Information (EPHI) and Personally Identifiable Information (PII) over these mediums without approved authorized security controls.

- Suspected security violations must be reported to the Enterprise Service Desk at 1-800-USAMITC or 907-TECH.

- User may not load software without written approval from the Information Management

Department and/or IA officials. Unauthorized software poses a great risk to the network. If you require software to be loaded you must contact the Enterprise Service Desk at 1-800-USAMITIC or 907-TECH.

- The usage rights of violators of the guidance specified in this memorandum or any other document or guidelines as referenced herein may be revoked at any time without warning. Furthermore, depending on the severity and/or frequency of the violation, disciplinary actions may be pursued under the Uniform Code of Military Justice for military personnel and appropriate civilian actions for civilian personnel. Contractors and or the contract can be terminated and are subject to local, state, and federal laws.

- The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.

- At any time, the government may inspect and/or seize data stored on this information system and **any device** attached to this information system.

Communications occurring on or data stored on any government IS or any device attached to the government IS are not private and may be disclosed or used for any U.S. Government authorized purpose. All IS are subject to routine monitoring and search.

- Security protections may be utilized on this IS to protect certain interests that are important to the government. For example, passwords, access cards, encryption or biometric access controls provide security for the benefits of the government. These protections are not provided for your personal use or privacy and may be modified or eliminated at the government's discretion.

- Use of ISs for unlawful or unauthorized activities such as file sharing of media, data, or other content that is protected by Federal or state law, including copyright or other intellectual property statutes.

- I will not modify the IS or software, or use of it in any manner other than its intended purpose, or adding user-configurable or unauthorized software such as, but not limited to, non-government instant messaging or Internet chat, collaborative environments, or peer-to-peer client applications.

- I will not attempt to strain, test, circumvent, or bypass network or IS security mechanisms, or to perform network (unless properly authorized) or keystroke monitoring.

- I will not physically relocate or make changes to configuration or network connectivity of IS equipment without proper authorization.

- I will not install non-Government-owned computing systems or devices without prior

authorization of the appointed Designated Approving Authority (DAA) including but not limited to USB devices, external media, personal or contractor-owned laptops, and MCDs.

- I will not release, disclose, transfer, possess, or alter information for non-official use as defined by AR 380-5.

- I will not share personal accounts and authenticators (passwords or PINs) or permit the use of remote access capabilities through Government provided resources.

- Disabling or removing security or protective software and other mechanisms and their associated logs from IS are prohibited.

- Employee-owned Information Systems (EOISs) are prohibited from storing, manipulating, or reading classified or sensitive information; this includes EPHI and PII. The use of and EIOS for ad-hoc (one-time or infrequent) processing of unclassified information is restricted and only permitted with the Information Assurance Manager (IAM), DAA, or Commander approval. If approved for ad-hoc use, EOISs processing official data will comply with all security provisions of this regulation. Computer owners will implement IA countermeasures required by this regulation, specifically Anti-Virus and IA software and updates, (personal firewall and Microsoft automatic patch updates). All processed data will be removed from the EIOS and personnel will sign compliance statements that the data was removed. Contractor-owned and operated ISs will meet all security requirements for government-owned hardware and software when operating on the Army Enterprise Infrastructure (AEI) or conducting official business. Remote access for remote management form EOISs is prohibited.

- I will not use personally owned removable media devices (thumb drives, PDAs, CDs, DVD, iPhones, iPads, etc…) on Government equipment, and for storing, or processing Government data. Only Government Furnished Equipment devices are permitted to connect to Government systems. All removable media must be labeled to the classification level of data contained on the device. Labels can be obtained from the Forms and Publication Office.

- At no time will non-government acquired/provided removable media be inserted into or connected to ANY Army computer system. I understand that connecting employee-owned removable media to any Army information system, computer or network for any purpose, including powering or charging a device, is expressly prohibited.

- WAMC employees are prohibited from use of unauthorized copies of software. Licensed software will be provided to all personnel who require it in connection with their work. Personnel who copy, use, or otherwise acquire unauthorized software are subject to disciplinary action. In addition, personnel will be aware that anyone illegally reproducing software may be subject to civil and criminal penalties.

- Modification of a workstation or software, use of it in any manner other than its intended

purpose, or adding user-configurable or unauthorized software such as, but not limited to, commercial instant messaging, commercial Internet chat, collaborative environments, or peer-to-peer client applications is prohibited.

- Army/MEDCOM approved collaboration tool is Defense Connect Online (DCO). The use of DCO chat is authorized. Use of other client-less Internet-based Capabilities, such as instant messaging, are only authorized with approval of the MEDCOM Certification Authority (CA).

- WAMC employs a variety of security controls within the WAMC information systems infrastructure. If an individual using WAMC IS resources is not in compliance with the above policy, the individual responsible will be held accountable for such non-compliance and may be subject to disciplinary or other corrective actions as appropriate. In some cases, individual actions may be subject to criminal or civil liability and result in a mandatory referral of the action to the U.S. Attorney or Judge Advocate General for disposition.

- Use of peer-to-peer software poses a serious risk to the Army Infrastructure and its use is strictly prohibited.

- I am accountable for ANY actions performed with my CAC card and pin number and that sharing this unique user information is prohibited. I will not use my CAC card and pin number to permit any other individual to access the WAMC network or my computer.

- I will use screen locks and log off the workstation when departing the area.

- I am prohibited to transmit information that contains profane or offensive language. I also understand that no information containing obscene or indecent material will be accessed, stored or transmitted using the WAMC network.

- I acknowledge my responsibility to use the WAMC network and IS for authorized or official government business ONLY and that I must use them in accordance with the provisions of the DoD, Army, and WAMC policy on the use of Government resources and communications systems. When in doubt, I will contact my supervisor for guidance.

- Only the Public Affairs Officer may authorize release of information identified as the WAMC's official position. I understand that when participating in unofficial forums, such as Internet chat rooms and News groups; I am prohibited from making or posting comments on any matter concerning Command policy, functions, responsibilities, or operations. I further understand that I may not initiate, be drawn into, or participate in discussions that are not required to accomplish official government business. If in doubt, I will contact my supervisor or the IA office for guidance.

4. I understand that the items listed below are considered by AR 25-2 as Prohibited Activities while using the IS.....

- Pornography or obscene material (adult or child)
- Copyright infringement (including the sharing of copyright material by means of peer-to-peer software)
- Gambling
- Transmission of chain letters (or replying to chain letters)
- Unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use
- Violation of any statute or regulation
- Hateful, harassing, or other antisocial behavior.
- Release of information about the Government that has not been approved for disclosure
- Disclosure of restricted information to unauthorized recipients
- Sending sensitive or classified information in clear text (unencrypted) over the Internet
- Hacking or attempting to hack into AIS
- Other inappropriate activities detrimental to the US Government

5. Sanctions for non-compliance. Results of policy violations will be handled in the following manner. Note any action can lead to criminal offenses covered by UMCJ and or the US Code.

First Violation The offender will come to the IA office for face-to-face confirmation, identification, and explanation of the incident with the Information Assurance Network Officer (IANO) or his/her designated representative. The offender will be required to sign this statement, sign the Acceptable Use Policy and complete remedial Cyber Awareness Challenge training both Step I & Step II. All forms will be kept on file with the IA office. Your account will be re-enabled at the direction of the IANO.

Second Violation The offender and Supervisor will come to the IA office for face-to-face confirmation, identification, and explanation with the IANO or his/her designated representative. The offender will be required to sign another statement with acknowledgement of the incident from the user's immediate Supervisor, offender will sign the Acceptable Use Policy and complete remedial Cyber Awareness Challenge training both Step I& Step II. All forms will be kept on file with the IA office. Your account will then be re-enabled at the direction of the Chief of IMD/WAMC CIO.

Third Violation The offender and Supervisor will come to IA office for face-to-face confirmation, identification, and explanation with the Chief of IMD/WAMC CIO or his/her designated representative. The offender will be required to sign another statement with acknowledgement of the incident from the user's immediate Supervisor, offender will sign the Acceptable Use Policy and complete remedial Cyber Awareness Challenge training both Step I & Step II. All forms will be kept on file with the IA office. Your account will then be re-enabled at the direction of the Hospital Commander.

6. Acknowledgement. *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 and 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 counter-intelligence 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 products 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 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 counter-intelligence 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 capture/seized privileged communications and data to ensure they are appropriately protected.

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

OFFICIAL:

STEVEN J. BREWSTER
COL, MC
Commanding

7. Signing Information. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to WAMC NETWORK information systems.

Department	Date
Last Name, First, MI	Rank/Grade
Signature	Phone Number
Supervisor Signature	Phone Number