ACCEPTABLE USE POLICY (AUP)
& ACKNOWLEDGEMENT OF RESPONSIBILITIES

User Acknowledgement

By signing this document, you acknowledge that you have read the requirements regarding use of the TAMC network and understand your responsibilities regarding these systems and the information contained in them. Additionally:

- By signing this document, you acknowledge and agree that when you access Department of Defense (DoD) information systems:
    - You are accessing a U.S. Government (USG) information system (IS) (which includes any devices attached to this information system) that is provided for U.S. Government-authorized use only.
    - You consent to the following conditions:
        - The 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 Counter-Intelligence (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 personnel 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, or privileged communications or data (including work products) that are related to personnel representation or service 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 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.

ACCEPTABLE USE POLICY (AUP)
& ACKNOWLEDGEMENT OF RESPONSIBILITIES

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality will be 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 protection 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 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.

    - In cases when the user has consented to content searching or monitoring of the 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.

User Name: _____ _____
(Last name, First, M-Rank/Grade) (Directorate / Division / Branch

User Signature: _____ **Date Signed:** _____
(YYYY / MM / DD)