## ACCEPTABLE USE POLICY AGREEMENT

**TYPE OF ACCOUNT:** (*check one*): ☒ **General User** (*Review Section I*) ☐ **Privileged User** (*Review Sections I & II*)

### I. GENERAL USER

1. **UNDERSTANDING AND CONSENT**. I understand, acknowledge and consent to the following:

a. I am accessing a U.S. Government information system (which includes any device attached to this information system) that is provided for U.S. Government authorized used only.

b. The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, Information Systems Security Monitoring, network operations and defense, personnel misconduct, law enforcement and counterintelligence investigations.

c. At any time, the U.S. Government may inspect and seize data stored on this information system.

d. 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.

e. This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests – not for my personal benefit or privacy.

f. I understand that access to a U.S. Government system or network is a revocable privilege, and that failure to comply with requirements is a violation of the trust extended to me and may result in one or more administrative or judicial actions such as, but not limited to: chain of command revoking access or user privileges; counseling; adverse actions under the UCMJ and/or criminal prosecution; discharge or loss of employment; security incident reporting; and/or revocation of security clearances and access.

2. **MINIMUM SECURITY RULES AND PROCEDURES**. I acknowledge the following rules and procedures:

a. I know I am subject to disciplinary action for violations or abuse of access privileges in accordance with Army Regulation 25-2 and other applicable regulations & laws.

b. I have completed the DOD Information Assurance Awareness Training. I will participate in any other required training programs directed by DOD, Department of Army (DA) or local policy.

c. I will protect the authenticator(s) (e.g. passwords, pass-phrases and pin numbers) at the highest level of classification processed on the system or network and will use any local or remote access privileges granted to me to perform authorized tasks or mission related functions only. I will never reveal the authenticator(s) to anyone, nor will I store them in electronic or written form. Additionally, I will use separate and unique passwords for all accounts across different domains of classification. If I feel my authenticator(s) has/have been compromised, I will immediately report it to my unit/directorate/activity Information Assurance Security Officer, Information Assurance Manager and servicing S-2/G-2.

d. I understand that I am the only authorized user of my assigned account and I am responsible for any and all activity that occurs while logged to the system on under my assigned User ID. I will use this assigned account and Army information systems (computers, systems and networks) only for authorized purposes.

e. I will use only authorized hardware and software. I will not download, install or use any personally-owned, commercial off-the-shelf or public domain hardware, software, shareware, freeware, file-sharing software (including MP3 music and video files), peer-to-peer software (e.g. Napster, Kazaa), games or devices on a U.S. Government system.

f. I will not connect any personal IT equipment (e.g. PEDs and PDAs, personal computers or digitally enabled devices) to my U.S. Government system or network without prior written approval of the system/network Designated Approving Authority (DAA).

g. I will not access, store or transmit prohibited content including, but limited to, pornography, chain-mail, bogus threats, copyrighted protected material, etc.

h. I will use only authorized U.S. Government collaboration tools. I will not use commercial collaboration tools (e.g. Google Docs), to include file sharing or peer-to-peer software. I will not use any unapproved Internet “chat” services. If a chat service is required, I will use my AKO account or other DOD or Army approved chat service.

i. I will utilize social media sites (e.g. Facebook, YouTube, etc.) only as authorized by job or duty description; for official government purposes to be, or represent, official opinion or content; to conduct official business; or to release official agency information or other official communication. I may establish and use personal accounts only within a personal capacity. Personal accounts must have no connection to official agency sites and must not appear to be, or represent, official opinion or content. My identity could be misused as the general public’s perception of official responsibility or openness. They cannot be used to conduct official business or release official agency information or any other official communication related to the job or government activities and Army policy restricts the use of government systems to access and manage personal sites during official duty hours.

j. I will not access, alter, change, configure or use operating systems or programs, except as specifically authorized. I will not attempt to strain, test, circumvent, perform network line monitoring, or conduct keystroke monitoring. I will not attempt to bypass or defeat system or network security controls, or modify and/or delete system log files.

k. I will not modify or turn off the operating system password protected screen saver. I will remove my CAC from the system during periods of temporary nonuse when departing the immediate area and at the end of the duty day.

l. I will not divulge Personally Identifiable Information (PII) to anyone without a valid need-to-know. I will not remove materials containing PII from the workplace without proper authorization. I will encrypt all email correspondence and attachments containing PII. If I receive email containing PII that isn't encrypted, I will notify my unit/directorate/activity Information Assurance Security Officer.

m. I will apply the principles of Data at Rest (DAR) protection equivalent to the level of sensitivity of the information required to be protected. I will not enter information into a system if the information has a higher classification than that for which the system is rated. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by my unit/directorate/activity Information Assurance Security Officer. I will ensure that all desktop and mobile computing devices I possess (laptop, PDA, Blackberry, etc.) have an approved DAR solution installed, configured and in use.

n. I will follow procedures to report security violations and incidents; abnormal behavior; system or application errors; suspicious activity; chain e-mails; spam; virus warnings; missing equipment; or the presence of unknown installed programs in accordance with local policy. I will immediately report any discrepancies in system operations following any anti-virus definition update, protective security application configuration, system update, or failures to my unit/directorate/activity Information Assurance Security Officer.

o. I understand that systems are the property of the Army and are subject to automated or manual inspections in the conduct of normal administrative tasks including, but not limited to; security compliance; system configuration; review of authorized and unauthorized software; illegal or prohibited information; personal usage; policy violations; backup and recovery; or information classification reviews to ensure that the use is authorized and the system is secure.

p. I will immediately report any suspicious output, files, shortcuts, links or system problems to my unit/directorate/activity Information Assurance Security Officer.

**3. SECRET INTERNET PROTOCOL ROUTER (SIPRNET)**. I acknowledge that if connected to the SIPRNET—

a. I understand my password is classified at the highest level of information (e.g. SECRET) processed on the system or network and I will protect that password at the same level.

b. I will not attempt to access or process data exceeding the authorized classification level for the U.S. Government system being used, or for which I do not have a "need to know". I understand that systems connected to the NIPRNET are not authorized to process classified information. I will not exchange any data (e.g., email) or media (e.g., CDs or other external media types) between unclassified (NIPRNET) and classified (SIPRNET) systems.

c. I will use page and paragraph classification markings and will protect all data and output at the classification of the data, system or network accessed until the information has been downgraded or declassified by authorized personnel using appropriate procedures. I understand that U.S. classified information must be marked and protected according to AR 380-5.

d. Classified removable media will be properly marked and will not be removed from the work area without written approval from the servicing Installation Security Office. If classified material must be physically transported outside the building, I will ensure I have a valid courier card and authorization to transport the material.

**4. PORTABLE ELECTRONIC DEVICES (PEDs).** I acknowledge that if I am issued PEDs:

a. I understand that PEDs include, but are not limited to, cell phones, pagers, personal digital assistants (PDAs) (e.g. Palm Pilots, Pocket PCs), laptops, memory sticks, thumb drives, and two-way radios.

b. I have completed the Portable Electronic Devices and Removable Storage Media training.

c. I will ensure FIPS 140-2 certified encryption tools are used to encrypt unclassified data-at-rest on PEDs.

d. I am responsible for keeping PEDs physically protected at all times. I will immediately report the loss or theft of devices to my commander/director.

e. I will turn off wireless capability on the device unless it is required and approved (e.g., travel).

f. I will ensure PEDs containing wireless connectivity, audio/video recording, or transmission capability are prohibited in areas where classified information is electronically stored, processed, discussed, or transmitted.

g. I will not discuss classified data over a PED that has not been approved for classified.

h. I will ensure that a personally owned PED will not be used to transmit, receive, store, or process U.S. Government information, and I will not connect it to a U.S. Government network.

i. I will make sure all PEDs assigned to me are made available for maintenance, upgrades, and scanning as needed by the installation IT provider.

**5. INFORMATION SYSTEMS ACCESS AND USAGE ACKNOWLEDGEMENT**.

a. 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:

(1) I consent to the interception, capture, and seizure of all communications and data for authorized purposes (including personnel misconduct, law enforcement, or counterintelligence investigations). 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 may otherwise apply.

(2) I understand that nothing in this AUP shall be interpreted to limit my 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 any information system, regardless of applicable privilege or confidentiality.

(3) I understand that 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, it functions to remind me of the conditions that are set forth in this User Agreement, regardless of whether summarized, fully detailed, or expressly referenced.

(4) I understand that I may be subject to disciplinary action for any violation or abuse of access privileges. Military and civilian personnel may be subject to punitive and/or administrative action if knowingly, willfully or negligently compromising, damaging, or placing U.S. Government information systems at risk by not ensuring implementation of federal, DOD and Army policies and procedures.

(5) I will take reasonable steps to identify such communications or data that I assert is protected by any such privilege or confidentiality. However, the 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.

(6) 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. I will seek personal legal counsel on such matters prior to using an information system if I intend to rely on the protections of a privilege or confidentiality.

(7) A 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.

(8) 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.

b. In cases when I have 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.

c. I have read the foregoing requirements regarding the access of U.S. Government systems and networks. I understand and acknowledge the responsibilities associated with accessing and protecting the information contained therein.

**II. PRIVILEGED USER**

**1. UNDERSTANDING AND CONSENT**. I understand, acknowledge and consent to the following:

a. I am responsible for all requirements stated in Section I above.

b. I am responsible for all actions taken under my administrative, root or superuser account(s) and understand that the exploitation of this account would have catastrophic effects to all networks for which I have access. I will only use the privileged access granted to me to perform authorized tasks for mission related functions. I will use my general user account at all other times.

c. I will protect the administrative, root or superuser account(s) and authenticator(s) to the highest level of data or resource it secures.

d. I will not share the administrative, root or superuser account(s) and authenticator(s) entrusted for my use.

e. I will not create or elevate privileged rights of others, share permissions to information systems not authorized, nor allow others access to information systems or networks under my privileged account.

f. If I work in a capacity where I have rights to remotely log into users' systems, I will ensure they are positively informed of my presence prior to taking any actions on their system.

**III. REQUESTOR**

| **LAST NAME, FIRST NAME, MI** | **RANK/GRADE** | **DATE**<br>201703 |
|---|---|---|
| **SIGNATURE** | **ORGANIZATION**<br>HQ IMCOM/ | **TELEPHONE**<br>210-466- |