ARMY IT USER ACCESS AGREEMENT

The requirements in this IT User Access Agreement are consistent with the policy established in Army Regulation 25-2, Army Cybersecurity; the proponent agency is OCIO.

PART I

ACKNOWLEDGEMENT AND CONSENT

1. Acknowledgement. By signing the user agreement, the user acknowledges and consents that when they 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.

2. Consent.

a. You 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 (PM), 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, 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.

(4) 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.

b. 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) 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.

(2) 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 or 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.

(3) 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.

(4) 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.

(5) The 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.

(6) 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 or seized privileged communications and data to ensure they are appropriately protected.

(7) 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, (that is, 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.

(8) 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.

PART II

INFORMATION SYSTEM ACCESS

1. Understanding. The user understands that they have the primary responsibility to safeguard the information contained on the system being accessed from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use. Any use of Army Information Technology (IT) is made with the understanding that the user will have no expectation as to the privacy or confidentiality of any electronic communication, including minor incidental personal uses.

2. Access. DoD policy states that Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems), when use of such systems and equipment is paid for by the Federal Government, will be for official use and authorized purposes only. Official use includes emergency communications and communications necessary to carry out the business of the Federal Government. Authorized purposes include brief communications by employees while they are traveling on Government business to notify family members of official transportation or schedule changes. Authorized purposes can also include limited personal use established by appropriate authorities under the guidelines of the DoD Regulation 5500.7-R, para. 2-301 "Joint Ethics Regulation."

a. Internet Access. Internet access is intended primarily for work related purposes.

(1) The user will not circumvent any filters or blocks to gain access to restricted sites.

(2) If denied access to a particular website, needed for official or authorized use, the user will follow procedures on the "blocked website" notification to request the site be unblocked.

(3) The user will not use Army IS for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

(4) The user will not inflict harm through the use of electronic communication – the transfer of information (signs, writing, images, sounds, or data) transmitted by

computer, phone, or other electronic device. Examples include harassment, bullying, hazing, stalking, discrimination, retaliation, or any other types of misconduct that undermines dignity and respect.

b. Email.

(1) The user will adhere to the email practices as outlined in AR 25-1 or your local command.

(2) The user will properly report chain email, spam, and virus warnings by following the reporting procedures outlined by your local command.

(3) The user will not provide personal or official information if solicited by email

(4) The user will not use personal, commercial email to conduct official government business.

(5) The user will not auto-forward email from official government email to a commercial or personal email accounts.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing. If the user knowingly threatens or damages an Army Information System (IS) or communications system (for example, hacking or inserting malicious code or viruses) or participates in unauthorized use of Army network(s), the user will have their network access suspended or terminated.

4. Secret Classified Information Processing.

a. The SIPRNet is the primary classified IS for the Department of the Army. SIPRNet is a United States DoD system and approved to process SECRET collateral information.

(1) SIPRNet provides classified communication to external DoD organizations and other U.S. government agencies via electronic mail.

(2) The SIPRNet is authorized for SECRET or lower- level processing in accordance with the DoD Connection Approval Process (CAP).

(3) The classification boundary between SIPRNet, and NIPRNet requires vigilance and attention by all users.

(4) The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the SIPRNet is a security violation and will be investigated and handled as a security violation or as a criminal offense.

5. Unclassified Information Processing.

a. The NIPRNet is the primary unclassified information system for the Department of the Army. NIPRNet provides unclassified communication to external DoD and other United States Government organizations. Foreign Nationals may only access the network with authorizing official (AO) approval. Any release of Secret information on NIPRNet is a security violation and will be investigated and handled as a security violation or as a criminal offense.

b. NIPRNet is approved to process CUI, UNCLASSIFIED, SENSITIVE information in accordance with the DoD Connection Approval Process (CAP). It is not authorized to process confidential classification.

c. The NIPRNet and the Internet, as viewed by the Army, are synonymous. Email attachments are vulnerable to interception as they traverse the NIPRNet and Internet.

6. Public Key Infrastructure (PKI) Use.

a. Public Key Infrastructure provides a secure computing environment utilizing encryption algorithms (Public/Private-Keys).

b. Token/Smart Card (or CAC). The Cryptographic Common Access Card Logon (CCL) is now the primary authentication mechanism for all Army users (with very few exceptions). This is a two phase authentication process. First, the CAC is inserted into a middleware (reader), and then a unique user PIN number provides the validation process.

c. Digital Certificates (Private/Public Key). The CAC is used as a means to sending digitally signed e-mail and encrypted e-mail.

d. Private Key (digital signature), should be used whenever e-mail is sent, with the exception when sending to non-government. The digital signature provides assurances that the integrity of the message has remained intact in transit, and provides for the non-repudiation of the message that the sender cannot later deny having originated the e-mail.

e. Public Key is used to encrypt information and verify the origin of the sender of an email. It must be used to send sensitive information, information protected by the Privacy Act of 1974, and Information protected under the Health Insurance Portability and Accountability Act (HIPAA).

7. Minimum Security Rules and Requirements.

a. As an information system user, the following minimum security rules and requirements apply.

(1) The user is not permitted access to an information system unless in complete compliance with the DoD and Army personnel security requirements for operating in a SECRET (SIPRNet) or UNCLASSIFIED (NIPRNet) environment.

(2) The user must complete the approved DoD Cyber Awareness Challenge training at https://cs.signal.army.mil (primary site) or https://jkosupport.jten.mil/Atlas2/page/login/Login.jsf. Large groups can use the DoD Facilitator's Guide training as a last option, and participate in all training programs as required (inclusive of threat identification, physical security, IT User Access Agreement policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access. The user understands that the initial training certificate will expire one year from the date that the training is successfully completed and that the completion of annual refresher training is required (in accordance with AR 25-2).

(3) The user will use only authorized hardware, firmware, and software. The user will not install or use any personally owned hardware, software, firmware, shareware, or public domain software on Army IT without prior authorization of the AO.

(4) The user will not introduce executable code (such as, but not limited to, .exe, .vbs, or .bat files) to the IS without authorization by the AO, nor will they write malicious code.

(5) The user will use virus-checking procedures before uploading or accessing information from AO authorized removable media (for example, diskette, Universal serial bus [USB] device, compact disk, or secure digital memory card) to an Army IS. The user will not attempt to access or process data exceeding the authorized IS classification level. Ensure proper classification markings, storing, transportation and destruction of all SIPRNET CDs/DVDs.

(6) The user will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

(7) The user will safeguard and mark with appropriate classification level on all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

(8) The user is responsible for removing their hardware PKI Token and ensuring that their computer has logged off prior to departing the area.

(9) The user will not utilize ARMY or DoD-provided ISs for commercial financial gain or illegal activities.

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

(11) The user will immediately report any suspicious output, files, or system problems to the information systems security officer (ISSO) and follow local Incident Reporting Plans. All activities will cease on the system.

(12) The user understands that monitoring of an information system will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.

(13) The user understands that unauthorized use or abuse of DOD and Army telecommunications, unified capabilities (UC), and computing systems (including telephone, email systems, DOD mobile devices, web services, or other systems) may subject users to administrative, criminal, or other adverse action.

(14) The user understands that Army IT resources will not be used in a manner that would reflect adversely on the Army, such as chain letters; unauthorized advertising, soliciting or selling; uses involving gambling or pornography; uses that violate statute or regulation; or other uses that are incompatible with public service. The user understands that it is their duty to immediately report all Cybersecurity related events, potential threats, vulnerabilities, and compromises or suspected compromises involving Army IT resources to the appropriate ISSO.

(15) The user understands that they are responsible for any activity conducted using their account. The user understands that they may only use the account to which they are assigned and may not allow others to use their account, or permit the use of remote access capabilities through Government provided resources with any unauthorized individual. The user's password or PIN is not to be shared with anyone, including the supervisor. Users are responsible for taking reasonable precautions to maintain the security of their accounts and the data to which they are authorized access.

(16) The user must not directly access, download or view emails and email attachments containing or labeled as classified or unclassified sensitive information (for example, Controlled Unclassified Information) from a device, equipment, system or network (for example, cellphone, tablet, computer) not specifically authorized to process such information – either directly or through a website (for example, webmail) – unless this is done in a formally authorized and secured manner (for example, virtual environment, secure viewing application, sandbox application, secure thin client) that prevents such information from being either temporarily or permanently stored on the device, equipment, system, or network.

b. Users of Army furnished collaboration technology, or with virtual access to official government information, will not conduct official government business, in close proximity to Self-Monitoring, Analysis, and Reporting Technology (SMART) Internet of Things (IoT) devices and Intelligent Personal Virtual Assistant (IPVA) applications, without appropriate security measures in place. Examples of appropriate security measures include turning off SMART IoT devices, disabling the “audio” access and

"recording" functions from SMART IoT devices and IPVAs, or moving far enough away from their listening and viewing range.

8. The user will adhere to the following requirements regarding the use of social media.

a. Users will utilize social media sites only as authorized by job or duty description, for official government purposes, to conduct official business or to release official agency information or other official communication.

b. Users 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. Users recognizes that their identity could be misused by the general public's perception of their acting in official responsibility or openness. Users cannot use personal accounts to conduct official business or release official agency information or any other official communication related to the job or government activities.

c. Users recognize it is their responsibility to ensure that they are not giving the false impression that they are acting in an official capacity when using government office equipment for non-government purposes. If there is expectation that such a personal use could be interpreted to represent an agency, then an adequate disclaimer must be used.

d. Users understand the use of government systems to access and manage personal sites during official duty hours is strictly prohibited.

9. The user will adhere to the following requirements regarding political activism:

a. Users will not use the Army IS to engage in political activity while on duty (on pay status, other than paid leave, or representing the government in an official capacity) or in the workplace.

b. Users will not engage in political activity in an official capacity at any time. This includes using an official email account or a social media account created for use in an official capacity to engage in political activity.

c. Users will not use the Army IS to suggest, solicit or receive political contributions at any time.

d. Users will not use the Army IS to engage in political transmissions, to include transmissions that advocate the election of particular candidates for public office.

10. When a user is issued a mobile device, the issuing officer will provide a separate agreement to sign.

PART III

1. Acknowledgement.

a. I have read, understand, and agree to abide by the responsibilities and requirements for IT usage and information handling in accordance with this agreement.

b. I have read, understand and agree to the notice of privacy rights, and consented to monitoring and searches in accordance with this agreement.

c. I have read, understand, and accept that violations of my responsibilities, unacceptable use of IT, or mishandling of information, may be punishable by administrative or judicial sanctions, may result in revocation or suspension of authorized access, may require remedial training in order to regain access, or may negatively influence adjudication decisions of security clearances.

FCoE NCOA	
Organization/Division/Office Symbol	Military/civilian/Contractor/FN
Last Name, First, MI	Date
Signature	

REFERENCES

1. All Army Activities (ALARACT) 014/2017 (Professionalization of Online Conduct), 23 February 2017
   (http://www.apd.army.mil)

2. Army Regulation (AR) 25-1 (Army Information Technology), 15 July 2019
   (http://www.apd.army.mil)

3. Army Regulation (AR) 25-2 (Army Cybersecurity), 4 April 2019
   (http://www.apd.army.mil)

4. CNSSI (Committee on National Security Systems Instruction) 1300 (Instruction For National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25), October 2009
   (http://www.hsdl.org)

5. CNSSP (Committee on National Security Systems Policy) 25, (National Policy for Public Key Infrastructure in National Security Systems), 11 December 2017
   (http://www.cnss.gov)

6. Department of Defense Chief Information Officer Memorandum (Department of Defense Commercial Mobile Device Implementation Plan) 15 February 2013
   (http://dodcio.defense.gov)

7. DoD 5220.22-M (National Industry Security Program Operating Manual (NISPOM)), February 2006
   (http://www.dss.mil)

8. DoD 5500.7-R (The Joint Ethics Regulation), 17 November 2011
   (http://www.esd.whs.mil)

9. DoD 8570.01-M (Information Assurance Workforce Improvement Program, Change 4), 10 November 2015
   (http://www.esd.whs.mil)

10. DoDD 5205.16 (The DoD Insider Threat Program, Change 2), 28 August 2017 (http://www.esd.whs.mil)

11. DoDD 8140.01 (Cyberspace Workforce Management, Change 1), 31 July 2017 (http://www.esd.whs.mil)

12. DoDI 1020.03 (Harassment Prevention and Response in the Armed Forces), 8 February 2018 (http://www.esd.whs.mil)

13. DoDI 8500.01 (Cybersecurity), 14 March 2014 (http://www.esd.whs.mil)

14. DoDI 8510.01 (Risk Management Framework (RMF) for DoD Information Technology (IT), Change 2), 28 July 2017 (http://www.esd.whs.mil)

15. DoDI 8530.01 (Cybersecurity Activities Support to DoD Information Network Operations, Change 1), 25 July 2017 (http://www.esd.whs.mil)

16. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 4 (Security and Privacy Controls for Federal Information Systems and Organizations), 22 January 2015 (http://csrc.nist.gov/publications)

17. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a (Assessing Security and Privacy Controls for Federal Information Systems and Organizations: Building Effective Assessment Plans), 18 December 2014 (http://csrc.nist.gov/publications)