ARMY IT USER AGREEMENT

The requirements in this IT User 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 this user agreement, the user acknowledges and consents that when accessing Department of Defense (DoD) Information Systems (IS) the user is accessing a U.S. Government (USG) IS. (Which includes any device attached to the IS that is provided for USG authorized use only.)

2. Consent.

a. The user consents to the following conditions:

(1) The USG routinely intercepts and monitors communications on the IS 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 USG may inspect and seize data stored on the IS.

(3) Communications using, or data stored on the IS, is not private, is subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

(4) The IS includes security measures (e.g., authentication and access controls) to protect USG interests — not for the user's personal interests or privacy.

b. Notwithstanding the above, using an IS does not constitute consent to PM, LE, CI investigative searching or monitoring of the content of privileged communications or data (including work products) 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.

(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 USG actions for purposes of network administration, operation, protection, defense, or for COMSEC. This includes all communications and data on an IS, 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 PM, LE, or CI investigation). However, consent to interception, capture or seizure of communications and data is not consent to the use of privileged communications or data for PM, LE, or CI investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(3) Whether any communications or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with (IAW) 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.

(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 USG is authorized to take reasonable actions to identify such communications 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 communications 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 USG 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 PM, LE, or CI 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 USG may, solely at its discretion and IAW DoD policy, elect to apply a privilege or other restriction on the USG’s otherwise-authorized use or disclosure of such information.

(8) All the above conditions apply regardless of whether the access or use of an IS includes the display of a Notice and Consent Banner (“banner”). When a banner is used, its function is 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

IS 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 communications, 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 unblocking of the site.

b. Email.

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

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

(3) The user will not provide personal or official information if solicited by email from unknown sources or senders.

(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 any commercial or personal email accounts.

3. Records Management.

a. The user acknowledges that the management of records data on their government furnished device is their responsibility and their organization's and not the Mobility Program Office. It is their responsibility to follow the policy and guidance of DoD Instruction 5015.02, "DoD Records Management Program" and Army Regulation 25-400-2 "Army Records Management Program" and DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)" when creating, maintaining, and dispositioning records on behalf of the Army.

b. The user acknowledges compliance with all applicable preservation notices and litigation holds and will ensure their supervisor, legal and local records management official knows the location of any records that are subject to litigation, Freedom of Information Act, Audit or Congressional inquiry prior to the completion of their out-processing.

4. Training.

a. The user acknowledges that they must complete records management training at https://www.lms.army.mil within 60 days of employment and complete refresher training annually in IAW NARA Bulletin 2017 – 01.

b. The user acknowledges that they must complete initial and annual refresher CUI education and training at https://www.cdse.edu/Training, IAW DoD Instruction 5200.48.

c. The user acknowledges that they 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 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, IAW AR 25-2.

5. 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.

6. The user will not inflict harm using electronic communications – the transfer of information (signs, writing, images, sounds, or data) transmitted by computer, phone, or other electronic devices. Examples include harassment, bullying, hazing, stalking, discrimination, retaliation, or any other types of misconduct that undermines dignity and respect.

7. 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 IS (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.

8. Secret Classified Information Processing.

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

(1) The SIPRNet provides classified communication to external DoD organizations and other USG agencies via electronic mail.

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

(3) The classification boundary between the SIPRNet, and the 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 information classified as TOP SECRET information or above through the SIPRNet, is a security violation and will be investigated and handled as a security violation or as a criminal offense.

9. Unclassified Information Processing.

a. The NIPRNet is the primary unclassified IS for the Department of the Army. The NIPRNet provides unclassified communication to external DoD and other United States Government organizations. Any release of information classified SECRET or above on the NIPRNet, is a security violation and will be investigated and handled as a security violation or as a criminal offense.

b. The NIPRNet is approved to process CUI, UNCLASSIFIED, SENSITIVE information IAW the DoD Connection Approval Process (CAP). It is not authorized to process confidential, SECRET, or TOP SECRET information.

c. The NIPRNet and the Internet, as viewed by the Army for the purposes of email

transmission, are synonymous. Email attachments are vulnerable to interception as they traverse the NIPRNet and Internet.

d. Foreign Nationals (FNs) may only access the network IAW AR 25-2 and DA PAM 25-2-18 (Foreign Personnel Access to Information Systems).

10. 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 to send digitally signed email and receive encrypted email.

d. Private Key (Digital Signature), will be used whenever e-mail is sent. 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 so that the sender cannot later deny having originated the email.

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

11. Minimum Security Rules and Requirements.

a. As an IS user, the following minimum-security rules and requirements apply.

(1) The user is not permitted access to an IS unless in complete compliance with the DoD and Army personnel security requirements for operating in the appropriate classification environment.

(2) The user will use only authorized hardware, firmware, and software.

(3) 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, universal serial bus [USB] device, compact disk, or secure digital memory card) to an Army IS.

(6) The user will not attempt to access or process data exceeding the authorized IS classification level.

(7) The user will ensure proper classification markings, storage, transportation and destruction of all media, including but not limited to the SIPRNet CDs/DVDs.

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

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

(10) The user is responsible for logging into their accounts at least once every 30 days to keep the account active. Unused accounts will be disabled or removed from the system after 35 days of inactivity IAW Windows 10 Security Technical Implementation Guide (STIG) V-220711.

(11) The user is responsible for removing their hardware PKI Token and ensuring that their computer is locked when leaving the device unattended and logged off at the end of the workday.

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

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

(14) 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.

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

(16) 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 actions.

(17) 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, IAW the organization incident response plan.

(18) 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.

(19) 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 (e.g., SMART phone, SMART watch, SMART TV, tablet, laptop, computer, speaker, web cameras, microphones, intercom/speaker capabilities, other automated listening/recording devices, voice to text and automated assistants such as Alexa, Siri, Cortana, Google’s Assistant Home, Mykie, Bixby, and networked devices etc.), 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.

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

13. Political Activities. 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, make 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 candidates for public office.

14. 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 this user agreement and understand and agree to:

(1) Abide by the responsibilities and requirements for IT usage and information handling IAW this agreement.

(2) The notice of privacy rights and consented to monitoring and searches IAW this agreement.

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

c. I understand that the user agreement must be signed annually at https://cs.signal.army.mil.

Organization/Division/Office Symbol	Military/Civilian/Contractor/FN
Last Name, First, MI	Date
Signature	

REFERENCES

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

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

3. Army Regulation (AR) 25-400-2 (Army Records Management Program), 18 November 2022 (http://www.apd.army.mil)

4. CNSSI (Committee on National Security Systems Instruction) 1300 (Instruction for National Secret Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25), 6 January 2022 (https://www.cnss.gov)

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. Code of Federal Regulations (National Industry Security Program Operating Manual (NISPOM)), Part 117 of Title 32, 21 December 2020 (https://www.ecfr.gov)

7. Defense Information System Network (DISN) Connection Process Guide (CPG), version 6.1, August 2023 (https://dod.cyber.mil)

8. DoD 5500.7-R (The Joint Ethics Regulation Change 7), 17 November 2011 (http://www.esd.whs.mil)

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

10. DoDD 8140.01 (Cyberspace Workforce Management, Change 1), 5 October 2020 (http://www.esd.whs.mil)

11. DoDI 1020.03 (Harassment Prevention and Response in the Armed Forces, Change 2), 20 December 2022 (http://www.esd.whs.mil)

12. DoDI 1035.01 (Telework and Remote Work), 8 January 2024 (http://www.esd.whs.mil)

13. DoDI 5015.02 (DoD Records Management Program Change 1), 17 August 2017
(http://www.esd.whs.mil)

14. DoDI 5200.48 (Controlled Unclassified Information (CUI)), 6 March 2020
(http://www.esd.whs.mil)

15. DoDI 8500.01 (Cybersecurity, Change 1), 7 October 2019
(http://www.esd.whs.mil)

16. DoDI 8510.01 (Risk Management Framework (RMF) for DoD Systems), 19 July 2022
(http://www.esd.whs.mil)

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

18. DoDM 8140.03 (Cyberspace Workforce Qualification and Management Program), 15 February 2023
(http://www.esd.whs.mil)

19. National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 53 revision 5 (Security and Privacy Controls for Information Systems and Organizations), 10 December 2020
(http://csrc.nist.gov/publications)

20. NIST SP 800- 53a revision 5, (Assessing Security and Privacy Controls for Information Systems and Organizations), 25 January 2022
(http://csrc.nist.gov/publications)

21. Department of the Army Pamphlet 25-2-18 (Foreign Personnel Access to Information Systems), 8 April 2019
(https://armypubs.army.mil)

22. NARA Bulletin 2017 – 01 (Agency Records Management Training Requirements), 29 November 2016
(https://www.archives.gov)

23. Windows 10 Security Technical Implementation Guide (STIG) V-220711, 10 March 2021
(https://www.stigviewer.com)