ALTESS Acceptable Use Agreement (AUP) for Visitors

1. **By signing this document**, you acknowledge and consent that when you access Department of Defense (DOD) Information Systems (ISs):

   a. You are accessing a U.S. Government (USG) IS (which includes any device attached to this IS) that is provided for U.S. Government-authorized use only.

   b. You consent to the following conditions:

      1) This U.S. Government routinely intercepts and monitors communications on this 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 (CO) investigations.

      2) At any time, the Government may inspect and seize data stored on this IS.

      3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, an may be disclosed or used for any U.S. Government-authorized purpose.

      4) This IS system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy.

      5) Notwithstanding the above, using an IS 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:

         i. 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 IS, regardless of any applicable privilege or confidentiality.

         ii. 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.

iii. 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 IS if the user intends to rely on the protections of a privilege or confidentiality.

iv. 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.

v. 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 to not negate any applicable privilege or confidentiality.

vi. 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.

vii. 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.

viii. All of 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, 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.

2. **Understanding**. I understand that I have the primary responsibility to safeguard the information contained in the A-WAN from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use. I will use Army information systems (computers, portable electronic devices (PEDs), systems, and networks) only for authorized purposes.

3. **Access**. Access to the ALTESS Network is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

4. **Revocability**. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

5. **Information processing**. The ALTESS Network is the primary unclassified information system for ALTESS.

   a. The ALTESS Network (A-WAN) is defined as the ALTESS Information System (IS) which contains all of its networked components and includes all Government owned PEDs. PEDs are portable ISs or devices with the capability of wireless or LAN connectivity. These include, but are not limited to, cell phones, pagers, personal digital assistants (PDAs) (for example, Palm Pilots, Blackberries, Pocket PCs), laptops and twoway radios. Current technologies (infrared, radio frequency, voice, video, microwave) allow the inclusion of several of these capabilities within a single device and dramatically increase the risks associated with IS and Network access.

   b. The A-WAN 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 http and https.

   c. The A-WAN is approved to process information considered as Sensitive but Unclassified (SBU) and handled and protected as For Official Use Only (FOUO).

   d. The U.S. Government IS, the A_WAN, the NIPRNet and the Internet, as viewed by ALTESS, are synonymous. Email and attachments are vulnerable to interception as they traverse the NIPRNet and Internet.

6. **Minimum security rules and requirements**. By gaining access to the A-WAN, the following minimum security rules and requirements apply:

a. I understand that I have no expectation of privacy with respect to any information, either official or personal, transmitted over, or stored within any Army IS to include information stored locally on the hard drive or other media including removable media or hand-held peripheral devices.

b. I understand that personnel are not permitted access to the A-WAN unless in complete compliance with the DoD and ALTESS personnel security requirements for operating in a SBU system-high environment.

c. I understand that I will complete the required user security awareness and PII training modules. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access. I further understand that this training is required annually. I will register and create an account with the Army Training and Certification Tracking (ATCTS) where I will track training and certifications.

d. I will generate, store and protect passwords, pins and pass-phrases for the IS I am accessing. Passwords will be in keeping with AR 25-2 with a minimum of fifteen (15) characters and will include a minimum of two each uppercase letters, lowercase letters, numbers and special characters. I am the only authorized user of this account. I will not store my passwords on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or on any magnetic or electronic media. I will not use my userid, common names, birthdays, phone numbers, military acronyms, call signs or dictionary words as passwords or pass-phrases.

e. I understand that commercial electronic mail (e-mail) accounts are prohibited for work-related communication.

f. I will not install or use any personally owned software, shareware or public domain software. I will not download file-sharing software (including music and videos files).

g. When sending e-mail, I will identify myself as a contractor within my e-mail signature, and I will use a standard signature block (if applicable).

h. I will not use Internet “chat” services including, but not limited to, America Online, Google, Microsoft Outlook express or Yahoo Instant Messenger on my Government Computer. If chat services are required, I will use my AKO account.

i. I will use virus-checking procedures before uploading or accessing information from any system, e-mail attachment or removable media, and insure virus definition files are no older than one week.

j. I will not alter, change, configure or use operating systems or programs, except as specifically authorized. This includes the Firefox browser which may only be authorized on a case-by-case basis with limited capabilities. The installation of Firefox add-ons is not authorized at any time.

k. I will not attempt to access or process data exceeding the authorized Information System (IS) classification level, nor will I transfer information from a classified IS to an unclassified IS.

l. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs or .bat files) without authorization, nor will I write malicious code.

m. I will not utilize Army or DoD provided ISs for commercial financial gain or illegal activities.

n. I understand that all maintenance will be performed by a Command-designated System Administrator (SA) only.

o. I will safeguard and mark with the 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.

p. I will never leave my IS unattended while I am logged on unless the IS is protected by CAC removal or other screen-locking protection.

q. I will immediately report any suspicious output, files, shortcuts or system problems to my designated Point of Contact (POC) and cease all activities on the system. Additionally, If I observe anything on the system I am using that indicates inadequate security, I will immediately notify my POC.

r. I will not connect any government or privately owned hardware such as PEDs, PDAs, personal computers, laptops, memory sticks (a.k.a. thumb drives), MP3 players, or mass storage devices to the Government IS. I understand any use of personally owned hardware is prohibited without the expressed written consent of the Information Security System Manager (ISSM).

s. I will address any questions regarding policy, responsibilities and duties my POC, and I will comply with all security guidance issued by my POC.

t. While at the ALTESS facility, I will not enter areas labeled as a “Restricted Area” unless I have a need and authorization to do so. Additionally, I will be aware of the TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections without first getting approval from the ALTESS IAM.

u. I understand that each IS is the property of the Army and is provided to me for

official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I realize that I should not store data on the IS that I do not want others to see.

v. I will observe the Data-At-Rest (DAR) policy in accordance with the US Army DAR Protection BBP.

w. I understand that, due to bandwidth restrictions, I should not routinely digitally sign or encrypt non-official emails. At a minimum I will:

1) Digitally sign emails sent from an Army owned system or account, which contain an active (embedded) hyperlink and/or attachment, requires data integrity, message authenticity or non-repudiation of sensitive information. Pure text references to web addresses, URL's or email addresses do not require digital signature, only active content and/or attachments.

2) Not digitally sign emails sent to non .mil addresses. I will not use an Active Directory Group Policy to automate 100% enforcement for digitally signing email. The non .mil recipients validate certificate using certificate revocation list checking (CRL). CRL retrieval by recipients outside the DoD will cause bandwidth issues. Automating digital signatures will increase CRL retrieval.

3) Encrypt sensitive information that includes, but is not limited to, For Official Use Only (FOUO), Sensitive but Unclassified (SBU) and Personally Identifiable Information (PII).

x. I understand that monitoring of the A-WAN will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or criminal prosecution. I understand that the following activities define unacceptable uses of an Army IS:

1) Use ISs for personal commercial gain or illegal activity (e.g., Ebay activity or the sharing of copyrighted material).

2) I will not forward chain e-mail or virus warnings. I will report chain e-mail and virus warnings to my POC.

3) Use ISs in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army or violates standards of ethical conduct.

4) Accessing, storing, processing, displaying, distributing, transmitting and viewing material that is: pornographic, threatening, harassing, political, racist, defamatory, vulgar, hate-crime related, subversive in nature, or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, national,

or international law.

5) Participate in on-line gambling or other activities inconsistent with public service.

6) Participate in, install, configure or use ISs in any commercial or personal distributed computing environment (DCE).

7) Release, disclose or alter information without the consent of the data owner, the Original Classification Authority (OCA) as defined by AR 380-5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office (PAO) or disclosure officer's approval.

8) Attempt to strain, test, circumvent, bypass security mechanisms or perform network or keystroke monitoring. Nor attempt to mask or hide my identity, or to try to assume the identity of someone else. I will not run "sniffer" or any hacker-related software on my IS.

9) Modify the system equipment or software, use it in any manner other than its intended purpose, introduce malicious software or code or add userconfigurable or unauthorized software (e.g., instant messaging, peer-to-peer applications).

10) Relocate or change IS equipment or network connectivity of IS equipment without proper security authorization.

11) Disable or remove security or protective software or mechanisms and their associated logs.

12) Use of Universal Serial Bus (USB).

7. **Acknowledgement -** I have read the above requirements regarding use of ALTESS access systems. I understand my responsibilities regarding these systems and the information contained in them. I affirm that I have the necessary security awareness training, baseline certification, and computing environment certification (IAW DoD Directive 8570) for the level of access being provided. I understand that I am subject to disciplinary action if I violate DoD computer policy.

_____ _____

Print Last Name, First, MI Date

Place Digital Signature in the provided box

ALTESS Acceptable Use Policy (AUP) for Visitors

CERTIFICATE OF NON-DISCLOSURE
Disclosure of protected or privileged information

Whoever, being an officer, employee or agent of the United States or of any department, agency or contractor thereof, publishes, divulges, discloses or makes known in any manner or to any extent not authorized by law, any information coming to him/her in the course of their employment or official duties, which information concerns or relates to the trade secrets or proprietary information of a non-Federal government entity; any information protected by the Privacy Act; any information subject to protection under the Freedom of Information Act; other law, regulation, or policy (including all privileged communications such as doctor-patient, attorney-client, etc.); any information protected under the classification system set forth in AR 380-5; or any other information protected by law or regulation (e.g., IG, AAA, CID); shall, in addition to any penalty imposed by said law or regulation, be subject to UCMJ, administrative or contract remedy enforcement.

CERTIFICATION

I have read the provisions herein, and I understand my responsibility not to disclose any matters connected with or pertaining to these provisions as they pertain to the ALTESS Information Systems except to persons theretofore listed as having a need to know.

_____
Date

_____
Print Last Name, First, MI

USER Digital Signature: