Acceptable Use Policy (AUP)

You must sign or digitally sign this form prior to issuance of a network userid and password. Initial Awareness Training must be completed prior to signing this agreement. IA Awareness training is found at https://ia.signal.army.mil/dodiaa/default.asp. The IA Awareness test located on the Fort Gordon website must be completed to fulfill the Awareness training requirement.

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

1. 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. You consent to the following conditions:

a. 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.

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

c. 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.

d. 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.

3. 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:

4. 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.

5. 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.

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. 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.

7. 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.

8. 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.

9. 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.

a. 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.

b. 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.

As a user of an information system, I will adhere to the following security rules

1. I will use Army information systems (computers, systems, and networks) only for authorized purposes.

2. I will not import any Government-owned software or install hardware on any Government computer (GC) (for example, client-workstation or server) without first getting written approval from my commander, SA, or IASO.

3. I will not load any software onto my GC, Government information technology (IT) system, or network without the approval of my commander, SA or IASO.

4. I will not try to access data or use operating systems or programs, except as specifically authorized.

5. I know I will be issued a user identifier (user ID) and a password to authenticate my computer account. After receiving them—

6. I will not allow anyone else to have or use my password. If I know that my password is compromised, I will report to my SA for a new one.

7. If my account is on a classified network, I understand that my password is classified at the highest level of information on that network, and I will protect it in the same manner as that information.

    a. I am responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when I am logged on a system with that account.

    b. If I have a classified account, I will ensure that my password is changed at least once every 90 days or if compromised, whichever is sooner.

    c. If I have an unclassified account, I will ensure that my password is changed at least twice a year or if compromised, whichever is sooner.

    d. I understand that if my password does not meet current DOD standards, I am to inform my SA.

    e. I will not store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or on any magnetic or electronic media unless approved in writing by the IASO.

    f. I will not tamper with my GC to avoid adhering to DOD password policy.

    g. I will never leave my classified GC unattended while I am logged on unless the GC is protected by a “password protected” screensaver.

    h. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.

8. I know that if connected to the Secret Internet Protocol Router Network (SIPRNET), my system operates at least in the U.S. Secret, “system-high” mode.

    a. Any magnetic media used on the system must be immediately classified and protected at the system-high level, regardless of the implied classification of the data (until declassified or downgraded by an approved process). In other words, any disk going into a Secret system is now classified as SECRET and must be handled accordingly.

    b. I must protect all material printed out from the SIPRNET at the system-high level until I or someone with the appropriate clearance personally reviews and properly classifies the material.

c. 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 the IASO.

d. If connected to the SIPRNET, only U.S. personnel with a security clearance are allowed unescorted access to the system.

e. Magnetic disks or compact disks will not be removed from the computer area without the approval of the local commander or head of the organization.

9. My local IASO has informed me of 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 SA or IASO. (If applicable)

10. I will scan all magnetic media (for example, disks, CDs, tapes) for malicious software (for example, viruses, worms) before using it on a GC, IT system, or network.

11. I will not transfer information using magnetic media from a classified system to an unclassified system.

12. I will not forward chain e-mail or virus warnings. I will report chain e-mail and virus warnings to my IASO and delete the message.

13. I will not run “sniffers” (utilities used to monitor network traffic, commonly used to Spy on other network users and attempt to collect their passwords) or any hacker-related software on my GC, Government IT system, or network.

14. I will not download file-sharing software (including MP3 music and video files), peer-to-peer software (i.e. Kazaa, Napster) or games onto my GC, Government IT system, or network.

15. I will not connect any personal IT equipment (for example, PEDs and PDAs (such as Palm Pilots), personal computers, and digitally enabled devices) to my GC or to any Government network without the written approval of my commander, SA, or IASO and IMO.

16. I will ensure that my anti-virus software on my GC is updated at least weekly.

17. I will not use Internet “chat” services (for example, America Online (AOL), Microsoft Network (MSN) Instant Messenger, Yahoo) from my GC. If chat service is needed, I will use my AKO account.

18. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify the site IASO. I know what constitutes a security incident and know that I must immediately report such incidents to the IASO.

19. I will comply with security guidance issued by my SA and IASO.

20. If I have a public key infrastructure (PKI) certificate installed on my computer (for example, software token), I am responsible for ensuring that it is removed when no longer required. If the certificate is no longer needed, I will notify my SA and the issuing trusted agent of local registration authority.

21. I know that my actions as a user can greatly affect the security of the system and that my signature on this agreement indicates that I understand my responsibility as a user requires that I adhere to regulatory guidance.

22. I know I am subject to disciplinary action if I violate DOD computer policy. For U.S. personnel, this means that if I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code or Code of Federal Regulations.

23. Acknowledgement: I have read the above requirements regarding use of Army in Europe access systems. I understand my responsibilities regarding these systems and the information contained in them.

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

Computer User
Signature _____ Date Signed _____

IAM/IASO Name
(Last name, First, M-Rank/Grade) _____ IAM/IASO
Signature _____