US AFRICA COMMAND Information Technology Acceptable Use and User Agreement

---

You must print and sign or digitally sign this form prior to network access. Initial Information Assurance Awareness Training must be completed prior to signing this agreement. IA Awareness training site: https://ia.signal.army.mil/DoDIAA/default.asp . The IA Awareness exam must be completed to fulfill the Awareness training requirements In Accordance With (IAW) DoDI 8500.2, para E 3.3.7.

Privacy Act Statement AUTHORITY: 5 U.S.C. 301; 10 U.S.C. 131.

PRINCIPAL PURPOSE(S): Identifies the user to the systems and devices as receiving usage and security awareness training governing use of the device and agreeing to use the devices IAW security policies.

ROUTINE USE(S): None.

DISCLOSURE: Voluntary; however, failure to provide the requested information may result in denial of issuance of access tokens.

USER INFORMATION:

Last Name:	
First Name:	

By signing this document, you acknowledge and consent that when you 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.

The consent to the following conditions:

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.

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

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

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

Notwithstanding the above, use of information systems 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.

Nothing in this document will 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.

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.

Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined IAW 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.

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.

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.

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 will take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

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 IAW DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

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 document.

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

1. I will use USG information systems and all connected devices for authorized purposes only and ensure only authorized personnel operate the equipment.

2. I will not use personal encryption systems or methods when transmitting communication.

3. I will comply with United States Africa Command (USAFRICOM) notices, instructions, manuals, and guides specific to the security of Information Systems.

4. I will complete initial, annual, and special training requirements within the compliance dates.

5. I will not install software or hardware on any Government computer (GC) or device without prior written approval from the Designated Approving Authority (DAA).

6. I will not attempt to access data, systems, devices, or use operating systems or programs, except as specifically authorized.

7. I understand I will be issued a user identifier (user ID) and password, token, or other method to authenticate and access the network and devices. Upon receiving access to the network . I will not share or allow use or access by another person or device using my authentication. If my access is compromised, I will report it immediately.

8. My account information for classified network authentication is classified at the highest level of information on that network, and I will protect it in the same manner as that information.

9. I understand there are two DoD Information Systems (IS), classified Secure Internet Protocol Router Network (SIPRNet) and unclassified (Non-secure Internet Protocol Router Network) (NIPRNet), and affirm I have the necessary clearance for access. If my clearance is withdrawn, I will not access these systems.

10. I will not participate in any actions prohibited by DoD 5500.07-R, Joint Ethics Regulation or any other DoD issuances.

a. I will not engage in prohibited political activity.

b. I will not use the system for personal financial gain such as advertising or solicitation of services or sale of personal property in non-DOD authorized systems (e.g., eBay), or stock trading (i.e., issuing buy, hold, and/or sell directions to an online broker). However, the Outlook sale folder is an authorized location where AFRICOM personnel may sale their personal items.

c. I will not conduct fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the Command.

d. I will not gamble, wager, or place bets using the network or devices.

11. I am responsible for all activity that occurs on or using my individual account or accounts I have access or authorization to use.

12. If I am a member of a group account, I am responsible for any unauthorized activity of that account while during my use.

13. If a password is used for authentication, I will ensure it is changed at least once every 60 days or immediately if compromised or disclosed to others.

14. I must use complex passwords that meet or exceed DOD standards.

15. I will not store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), on any magnetic or electronic media or in written form.

16. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the Help Desk by secure means.

17. I will not Introduce Classified or Controlled Unclassified Information (CUI) into a NIPRNet environment.

18. I will report any instance of Classified or CUI on NIPRNet to the Help Desk by secure means upon discovery.

19. I know that if connected to the Secret Internet Protocol Router Network (SIPRNet), my system operates 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). Any disk used in a SIPRNet system is immediately marked as SECRET and must be handled accordingly.

b. I must protect all material physically printed from the SIPRNet.

c. I will not enter, process, or aggregate information on a system of lower classification than required for the information.

d. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved for that system.

e. I understand and will enforce the requirement that only U.S. personnel with a valid and verified security clearance are authorized access.

20. I will not introduce any unauthorized code, Trojan horse programs, malicious code, worms, or viruses into the networks.

21. I will not access, store, process, display, distribute, transmit, or view material that is abusive, harassing, gender, bias, defamatory, vulgar, pornographic, profane, racist, promotes hate crimes, subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, state, federal, national, or international law.

22. I will not store, access, process, or distribute Classified, Proprietary, CUI, For Official Use Only (FOUO), or Privacy Act protected information in violation of established security and information release policies.

23. I will not tamper or attempt to circumvent device or network security settings or to avoid adhering to DOD policy.

24. I will not run sniffers, utilities, programs, devices, appliances, disks, ISOs (images), software, or websites designed to monitor, capture, scan, probe, spy, or inspect network traffic or attempt to collect passwords, data, or any potentially useful intelligence about the systems, network, or configuration of devices unless it is specifically part of my position description and authorized by the DAA.

25. I will not download, install, or run any software not specifically authorized by the DAA including file-sharing software, peer-to-peer software (i.e. Kazaa, Napster) or games onto my GC, Government IT systems, or networks.

26. I will not download or store unofficial files or files which potentially infringe on copyrights of music, photo, or video files.

27. I will not connect any personally owned Information Technology (IT) equipment including Human Interface Devices ((HID) monitors, keyboards, pointing devices, mouse substitutes), Personal Electronic Device ((PED) iPad, iPod, cellular phones, ETC), Personal Digital Assistant ((PDA) Palm, Symbian, iPAQ, ETC), computers, notebooks, laptops, tablets, or digitally enabled devices to GC or to any Government network without the written approval of the DAA.

28. I will not use unauthorized commercially based Internet chat or messaging services (America Online (AOL) Instant Messenger (IM), Microsoft Network (MSN) Instant Messenger, Yahoo, Skype, Facebook, Google+,Trillium, Google Chat, others) from my GC. Authorized chat services are limited to Army Knowledge Online (AKO), Defense Knowledge Online (DKO), Defense Connect Online (DCO), and Lync.

29. I will not leave any device unattended while I am logged on unless it is protected by a locked screensaver.

30. I will not attempt to mask or hide my identity from Government oversight or assume the identity of someone else while using Government networks or devices.

31. I will follow TEMPEST (Red/Black) separation requirements for system components and ensure metal wiring from disparate classified systems are not within 3 inches and processors of devices are not within 20 inches of one another.

32. I will not move hardware or alter communications connections without coordination with authorized network security personnel.

33. I will process all magnetic media (for example, disks, CDs, DVDs) through a Data Transfer Agent (DTA) before use.

34. I will not transfer information from a classified system to an unclassified or lower level system unless I am designated as a DTA.

35. I will not forward potential email chain letters, hoaxes, or virus warnings to other users and I will report suspected instances to the Help Desk.

36. I will digitally sign all emails which contain links, Uniform Resource Locator (URL), or attachments.

37. I will not use links, URLs, or attachments sent to me that are not digitally signed. If I receive an unsigned link or attachment, I will contact the sender to verify authenticity. I will type unsigned links/URLs into the browser and not click to activate the link in emails.

38. I will only attach files when file sharing locations are unavailable or not feasible (non-domain recipient).

39. I will handle all information IAW the USAFRICOM Critical Information List (CIL).

40. If I observe anything on the system which indicates inadequate security, malicious, or suspect activity, I will immediately notify the Help Desk.

41. I will comply with all security guidance.

42. If I have a public key infrastructure (PKI) certificate installed on my computer (software certificate), I will ensure that it is removed when no longer required and safeguard the certificate from disclosure. If the certificate is no longer needed, I will notify the issuing Trusted Agent (TA) or Local Registration Authority (LRA).

43. I understand my actions greatly affect the security of the system and I understand my responsibilities to adhere to guidance, policies, and best practices.

44. I will physically secure Government owned devices in transit and at rest. If a device is highly pilferable (notebooks, laptops) and possesses a Universal Security Slot (USS), a cable lock or alarm must be used.

45. I understand that a docking station is not a security device. I will ensure that unoccupied areas are locked and secured. I will anchor devices to a fixed object.

46. I will remove and secure removable device cards under lock and key.

47. I will ensure portable devices are labeled with a Return If Lost Address.

48. I will sign for and maintain responsibility under the property book system for assigned devices and maintain serial and model identification numbers.

49. I will use non-descript carrying cases and not publicly display a laptop case or highlight the manufacturer, organization, or military affiliation.

50. I will remain vigilant during air or rail travel, especially at security checkpoints. I will keep the device in sight at all times. Devices will never be placed in checked or unattended baggage.

51. I will never leave a device in a vehicle where it can be seen and will use a cable lock to securely mount it within the vehicle.

52. I will not leave devices unattended in public, meetings, conventions, or conferences.

53. I will immediately report the loss of a device.

54. I will ensure that only one connected interface (Wi-Fi or Wired or Cellular or Modem) is active at a time. All others will be disabled.

55. I will not circumvent security for matters of convenience.

56. I will use Virtual Private Network (VPN) technologies if network access is required. To protect the network, I will not use devices that connect by VPN to access non-government networks.

57. I will ensure that approved encryption products are in use for protecting data-at-rest on all mobile ISs.

58. I will use privacy screens in public facilities or during travel.

59. I will always log off and shut down the laptop system during travel and never use the sleep or hibernation modes.

60. When connecting wirelessly, I will use internet access through Cellular Wireless Broadband plans whenever possible. Wi-Fi as a secondary method. Other wireless systems (Bluetooth, IR, ETC) are prohibited.

61. I will ensure network quarantining and assessment (compliancy and contamination) procedures are completed before reconnection to the network after wireless use.

62. I will not store, process, or transmit classified information on a wireless system.

63. I will not transport or operate Cellular/PCS, Bluetooth, other RF or Infrared (IR) wireless devices in areas where classified information is discussed or processed.

64. I may be held responsible for damage caused to a Government systems, networks, or data through negligence or a willful act.

65. I understand my responsibility to appropriately protect and label all output generated under my account (including printed materials, magnetic tapes, floppy disks, and downloaded hard disk files).

66. I will not obtain, install, copy, paste, transfer, or use software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

67. I will not write, code, compile, store, transmit, or transfer malicious software code within the GS.

68.

Acknowledgement: I have read the above requirements regarding use of Government systems, networks, and devices. I understand my responsibilities and liability regarding

use of such systems and the safeguarding of information contained therein. I am subject to disciplinary action for violation of DOD, ARMY, or USAFRICOM policy. If I fail to comply, I am 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 administrative, disciplinary, or adverse action and/or civil or criminal prosecution for failing to comply with this agreement and/or DoD, Army, or USAFRICOM policies for the use of DoD information systems

---

Computer User

Last name, First, M-Rank/Grade _____

Signature _____

Date Signed _____

Or sign digitally below:
