

Army in Korea LandWarNet Acceptable Use Policy

17 June 2011

1. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained on the Army in Korea LandWarNet Classified and/or Army in Korea LandWarNet Unclassified networks from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

2. **Access.** Access to this/these network(s) is for official use and authorized purposes and as set forth in DOD 5500.7-R, "Joint Ethics Regulation", AR 25-2, "Information Assurance" (IA) or as further limited by this policy.

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

4. **Applicability.** The Army in Korea LandWarNet provides information processing service for both Classified and Unclassified. This Acceptable Use Policy applies to ALL DoD non-DoD personal who are required and authorized access to the Army in Korea LandWarNet Architecture.

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

a. 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.

b. 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.

(5) 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:

(a) 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.

Army in Korea LandWarNet Acceptable Use Policy

17 June 2011

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(f) 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.

(6) 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.

(7) 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 provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

6. Minimum security rules, requirements, and unacceptable use. As an Army in Korea LandWarNet Classified and/or Korea LandWarNet Unclassified system user, the following minimum security rules and requirements apply:

a. I will complete initial DoD IA awareness training and annual refresher training at the Fort Gordon, GA. IA training web site upon receiving access authorization to the Army in Korea LandWarNet.

Army in Korea LandWarNet Acceptable Use Policy

17 June 2011

b. I will use my common access card (CAC) for authentication on my government system and will not circumvent any installed security. I will remove my CAC when leaving my system for short periods of time and log off the system when departing the area for extended periods. I will perform a restart on my government system each work day to ensure that updates are applied. If required, I will generate, store, and protect passwords or pass-phrases. Passwords will be at least 15 characters, consisting of 2 each uppercase and lowercase letters, numbers and special characters. I will not share personal accounts and passwords or permit the use of remote access capabilities by any individual.

c. As a system user, I will not install or remove programs or hardware (government or personally owned), disable security configurations or audit logs, or alter operating system configurations. I will not attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring. I will not introduce any executable code nor will I write any malicious code.

d. I will use virus-checking procedures before uploading or accessing information from any system or device. I will use government provided virus-checking software and procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb drive, or any other removable and/or portable storage devices.

e. I will immediately report any suspicious output, files, shortcuts, or system problems to my unit Information Management Officer (IMO) and/or Information Assurance Security Officer (IASO) and cease all activities on the system. I will report all known or suspected security incidents, or violations of this acceptable use policy and/or AR 25-2 to the IASO, IMO, and Network Enterprise Center (NEC).

f. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the information system and will not disseminate it to anyone without a specific need to know. I will also include authorized official travel markings if I have been authorized to remove a government owned mobile computing device or data storage device. I will not attempt to access or process data exceeding the authorized information system classification level. I will access information only for which I am authorized access to and have the specific need-to-know.

g. I will not utilize Army or DOD provided IS for commercial financial gain or illegal activities. I will not use IS in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army, or violates standards of ethical conduct. I will not intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (spam) communications (LE/CI investigators, attorneys, or other official activities, operating in their official capacities only, may be exempted from this requirement.). I will not misuse government resources involving: pornography or obscene material (adult or child); copyright infringement (such as the sharing of copyright material by means of peer-to-peer software); gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.

7. Data-at-Rest Requirement.

a. I will identify Personally Identifiable Information (PII) and Sensitive Information (SI) data on any government owned system, mobile computing device, data storage device, or removable media in my possession. I will safeguard all government owned devices and data in my possession from loss, suspected loss, theft, unauthorized access, and person or multiple persons that do not have a need to know the information.

Army in Korea LandWarNet Acceptable Use Policy

17 June 2011

b. I will not remove any government owned computing device, data storage device, or removable media with PII or SI data from a government facility without approval of the Commander or Director in the grade of O6/GS15 and above in the chain of command.

c. I will encrypt all PII and SI sensitive data when removed from a government facility, or when contained within an electronic mail. To encrypt electronic mail, use the encrypt email solution built into Microsoft Outlook. To encrypt data on removable media, use the solution outlined in the Eighth Army Data-At-Rest (DAR) OPORD.

d. I will safeguard and protect PII and prohibit any uploading of PII on ALL USFK, Eighth Army, or any other SharePoint portals operating on the Army in Korea LandWarNet architecture.

e. I will not download any PII or SI to a non-government owned computing system or device.

f. I will immediately report the loss/suspected loss, compromised/suspected compromise, or discovery of PII and SI to the first O5 or GS14 in my chain of command and the local servicing NEC.

g. I will successfully complete the Personally Identifiable Information (PII) training prior to obtaining access to the Army in Korea LandWarNet (Unclassified and Classified) networks.

h. As an Authorized Official Traveler, I will complete the official traveler's checklist and obtain approval prior to removing a device from the facility IAW DAR Eighth Army OPORD. Upon returning, I will take the device to the IMO or Information Assurance Manager (IAM) to be scanned using an Army approved compliance scanning tool prior to being reconnected to the network

8. **Penalties.** I understand that violations of this agreement may be punitive in nature and punishable under Article 92 of the UCMJ or other administrative and criminal statutes. These violations are covered under AR 25-2, paragraph 1-1j.

9. **Acknowledgement.** I have read the above requirements regarding use of DoD and Eighth Army IS. I understand my responsibilities regarding these systems and the information contained in them.

Unit/Directorate/Division/Branch

Date

Last Name, First, MI

Rank/Grade/Contractor

Signature

Phone Number
