



DEPARTMENT OF THE ARMY
HEADQUARTERS 2D INFANTRY DIVISION
UNIT # 15041
APO AP 96258-5041

REPLY TO
ATTENTION OF

EAID-CG

FEB 28 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Letter #6-1, Information Assurance

1. Reference:

- a. DoD Directive 8570.01, Information Assurance Training, Certification, a Workforce Management, 23 March 2009.
- b. DoD Directive 8570.01-M, Information Assurance Workforce Improvement Program, 20 April 2010.
- c. AR 25-2, Information Assurance, 23 March 2009.
- d. ALARACT 051/2009 Army-Wide Network Security Focus Training Paragraph 3.A.I
- e. Army in Korea Unclassified LandWarNet (AKULWN) Army in Korea Classified LandWarNet (AKCLWN) Account Management Policy, 1 November 2011

2. Applicability. This policy applies to all personnel assigned, attached, or under the operational control of 2ID, including Department of Defense (DoD) civilian employees, invited contractors, technical representatives, and all family members. This policy supersedes the previous 2d Infantry Division (2ID) Command Policy #13, Information Assurance, dated 26 July 2010.

3. Policy. Information Assurance is a commander's program at all levels to implement and enforce. Commanders are charged with ensuring compliance with this policy letter. All personnel are charged with adhering to the specific policy guidance below.

a. All network and portable electronic devices connected to the network or stand alone will comply with the Department of the Army published Information Assurance Vulnerability Management (IAVM) directives and network security policies.

b. All privileged users will be trained and certified IAW DoDD 8570.01 and Army Best Business Practices.

c. All general users will complete the DoD Information Assurance Awareness Training, Portable Electronic Devices and Removable Storage Media, Phishing Awareness, Safe Home

EAID-CG

SUBJECT: Policy Letter #6-1, Information Assurance

Computing, Personally Identifiable Information (PII) courses as well sign the Korea LandWarNet (KLWN) Acceptable Use Policy (AUP).

d. All information assurance incidents whether suspected or in fact will be reported through their respective Information Assurance Security Officer (IASO) to the 2ID Information Assurance Manager (IAM).

e. All computers, laptops, portable electronic devices, and media will be Data-At-Rest (DAR) compliant, will be labeled with the appropriate level of classification, and will be government furnished equipment. Virtual Private Network (VPN) accounts require a DAR compliance check of portable electronic devices before use outside of the ordinary office environment.

f. No personally owned computer devices are allowed on the network regardless of situation.

g. All user accounts will be disabled upon Permanent Change of Station (PCS) or Expiration of Term of Service (ETS).

h. Personally Identifiable Information (PII) will be encrypted when contained within an e-mail or removed from a government facility. PII is any information about an individual that is private or intimate to the individual and as distinguished from information related solely to the individual's official functions or public life. This information includes, but is not limited to, any personal information which is linked or linkable to an individual, such as education, financial transactions, medical history, criminal or employment history, and information which can be used to distinguish or trace an individual's identity. Examples include social security numbers, date and place of birth, mother's maiden name, and electronic medical records.

i. No Peer-to-Peer downloads, Instant Messaging, or games are allowed on government furnished information systems if not explicitly approved by the 2ID IAM.

j. No unauthorized installation or removal of programs, disabling of security configurations or audit logs, altering system configurations, straining, testing, circumventing, or bypassing security mechanisms to include enabling the use of thumb drives unless explicitly permitted by the 2ID IAM.

4. Failure to follow any of the above procedures, proper security and regulations will result in immediate suspension of network access and privileges. These provisions may be punished as violations as follows:

a. Sanctions for civilian personnel may include, but are not limited to, some or all of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; suspension with or without pay; loss or suspension of access to IS or networks, and classified material and programs; any other administrative sanctions authorized by contract or agreement; and/or dismissal from employment. Sanctions for civilians may also include prosecution in U.S. District Court or other courts and any sentences awarded pursuant to such prosecution. Only civilian managers or military officials who have authority to impose the specific sanction proposed may award sanctions IAW AR 25-2.

EAID-CG

SUBJECT: Policy Letter #6-1, Information Assurance

b. Sanctions for military personnel may include, but are not limited to, some or all of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; and loss or suspension of access to IS or networks and classified material and programs. Sanctions for military personnel may also include any administrative measures authorized by service directives and any administrative measures or non-judicial or judicial punishments authorized by the Uniform Code of Military Justice (UCMJ).

c. Depending on the severity, the following must be completed to reactivate:

(1) First Offense – Memorandum signed by the first commander/director in the chain of command that is in the grade of O5, GS14/GG14/GM14 or higher. SM or Authorized user will retake training stated in paragraph 3.c. and resubmit the KLWN AUP. The account may be reactivated once the memo has been received and the requirements of paragraph 3.c. have been verified by the 2ID IAM.

(2) Second Offense – Memorandum signed by the first commander/director in the chain of command that is in the grade of O6, GS15/GG15/GM15, or higher. The account may be reactivated once the memo has been received and accepted by 2ID IAM, along with an automatic 15 day account suspension. SM or Authorized user will retake training stated in paragraph 3.c. and resubmit the KLWN AUP. The account may be reactivated once the memo has been received and the requirements of paragraph 3.c. have been verified by the 2ID IAM.

(3) Third Offense – Memorandum signed by the first General Officer or SES in the chain of command. The memorandum is submitted to the Army in Korea AKULWN/AKCLWN Designated Approving Representative (DAAR) and must state what actions and what corrective training was completed to prevent reoccurrence. The account may be reactivated once the memo has been received and accepted by 2ID IAM, along with an automatic 30 day account suspension.

5. Expiration. Policy Letter #6-1 is effective immediately and supersedes 2ID Policy Letter 13, Information Assurance, dated 26 July 2010. It remains in effect until rescinded or superseded.



EDWARD C. CARDON
Major General USA
Commanding

DISTRIBUTION:

A