



REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
HEADQUARTERS, EIGHTH ARMY
UNIT #15236
APO AP 96205-5236

EACG

APR 01 2013

MEMORANDUM FOR All Eighth Army Soldiers, Civilian Employees, and Contractors

SUBJECT: Eighth Army Command Policy Letter #60, Privileged Level User Violations

1. References:

a. Army Regulation 25-2, Information Assurance, 24 October 2007 (incorporating Rapid Action Revision, 23 March 2009)

b. Memorandum, HQDA, NETC-EST-IA, Subject: Implementation of Information Assurance Best Business Practice (IA BBP); 06-PR-M-0003: Privileged-Level Access Agreement Acceptable Use Policy (AUP), Version 1.0, 03 November 2006

c. Department of Defense (DoD) 8570.01-M, Information Assurance Workforce Improvement Program, 19 December 2005 (Change 3, 24 January 2012)

2. Purpose. To provide guidance and establish policy for privileged level user violations involving Army in Korea unclassified and classified systems and networks.

3. Background. Cyber is our newest warfighting domain. It is critical that we protect and defend our systems and networks to ensure our fight tonight mission readiness posture. Privileged level users are appointed, trained, and trusted to follow/enforce policy and ensure systems and networks remain secure. Commanders at all levels must ensure that Soldier, civilian, and contractor privileged level users understand their critical role and comply with Department of Defense and Department of the Army policy, standards and procedures.

4. Policy.

a. Privileged level user access is a privilege, not a right. Privileged level user violations are unacceptable and are a breach of trust between the individual, this organization, and the Army. Privileged level users who do not follow/enforce information assurance policies are negligent in their duties, introduce vulnerabilities, and place unnecessary risk to our mission. A compromise of privileged level access is as damaging to the readiness of a unit as losing a weapon or compromising COMSEC. A privileged level user is defined as a user with administrator access to systems or networks; access that is elevated above that of a normal user.

b. Commanders will initiate an investigation involving any report of a privileged level user violation (see enclosure 1) and ensure privilege level user access and access to classified information is suspended immediately pending the results of the investigation. Where violations of Army policy and/or negligence are founded, privileged level access will not be reinstated to the individual and an incident report will be opened in the Joint Personnel Adjudication System (JPAS) for adjudication and tracking purposes (see enclosure 2).

EACG

SUBJECT: Eighth Army Command Policy Letter #60, Privileged Level User Violations

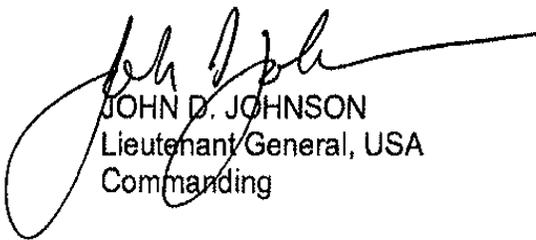
c. Commanders will ensure privileged level users are appointed in writing, have completed all Department of Defense and Department of the Army training and certification requirements, and sign a privileged level user access agreement.

d. Commanders must minimize the number of appointed privileged level users to balance these risks with operational requirements.

5. Proponent. The Assistant Chief of Staff, G6, Eighth Army is the proponent for this policy. The proponent can be contacted at commercial 011-822-723-2949 or DSN 315-723-2949.

2 Encls

1. Examples of PLU Violations
2. Punitive Measures Available to Commanders



JOHN D. JOHNSON
Lieutenant General, USA
Commanding

Enclosure 1

Examples of Privileged Level User Violations (but not limited to)

- Disclosure of administrative passwords to unauthorized individuals
- Unofficial web browsing and commercial email use while using their PLU account
- Subvert data protection schemes, gain, access, share, elevate permissions to data or systems for which not authorized
- Modify system settings to bypass enterprise security mechanisms (e.g. proxy settings to get around web site restrictions)
- Download of unauthorized software or files from unauthorized sources
- Install any hardware (e.g. wireless routers, switches, wireless peripherals) to include personal devices (e.g. Ipad, laptop) without NEC approval (e.g. Requirements Document (RD), Network Change Proposal (NCP))
- Install any software outside of the Army Gold Master baseline image (e.g. games, freeware, entertainment software) without NEC approval (e.g. RD, Authority to Connect (ATC)) except security patches and printer drivers for approved software/hardware
- Install unauthorized or malicious code, backdoors or hardware
- Obtaining, installing, copying, pasting, modifying, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade-secret, or license agreements
- Create or elevating access rights of others; share permissions to Information Systems for which they are not authorized; nor allow others access to IS or networks under a PLU account
- Employing, using, or distributing unauthorized encryption capabilities for official electronic communications
- Failing to 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 appropriate IA Workforce
- Violating their Non-Disclosure Agreement and Privileged Level Users Access Agreement
- Failure to ensure the security of systems under their purview when vulnerabilities are known to him/her
- Employing classified systems, network devices, or equipment on unclassified networks
- Disabling CAC or PKI Token Card enforcement registry settings on unclassified or classified systems without authorization from the NEC (e.g. remedy ticket)
- Enabling wireless access in registry settings on unclassified systems without NEC approval

Enclosure 2

Punitive Measures Available to Commanders

At a minimum, the following actions will be taken for privileged level users where negligence is founded (any Soldier, Army Civilian, Contractor, and Korean National (KN) Employee):

- Incident Report opened on individual in JPAS for Misuse of Information Technology
- Revocation of privileged level user appointment orders and account access

Measures listed below may be taken at the discretion of the Commander based on results of an AR 15-6 investigation where negligence is founded.

- Letter of admonishment or letter of reprimand (Army Civilians and KN Employees)
- Adverse performance evaluation (Soldiers, Army Civilians, KN Employees)
- Contractor Discrepancy Report sent to Contracting Officer (Contractor)
- Written reprimand in accordance with AR 635-200, Paragraph 1-18b (Soldiers)
- UCMJ action for violation of AR 25-2, a punitive regulation (Soldiers)
- Bar to reenlistment in accordance with DA Form 4126-R (Enlisted Soldiers)
- Recommend reclassification of MOS due to disciplinary actions which adversely affect the soldiers' ability to perform MOS (Enlisted Soldiers)