DEPARTMENT OF THE ARMY
HEADQUARTERS, III CORPS AND FORT HOOD
1001 761ST TANK BATTALION AVENUE
FORT HOOD, TEXAS 76544-5000

COMMAND POLICY
NEC-01

REPLY TO
ATTENTION OF

NETC-SFB-DE

02 NOV 2009

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Computer Network Security

1. REFERENCE. AR 25-2, Information Assurance, 24 October 2007.

2. APPLICABILITY. This policy applies to all Fort Hood units and tenant activities that utilize computer systems on the Fort Hood network.

3. POLICY. In order to assure security of the Fort Hood network, commanders, senior executive and managers will ensure compliance with the following:

a. All Installation Local Area Network (ILAN) users must log into the NASW domain.

b. All network devices, whether wired or wireless, connected to the network or standalone, will comply with the Department of the Army published Information Assurance Vulnerability Management (IAVM) directives and network security policies.

c. All computers, laptops and media will be Data-At-Rest compliant, will be labeled with the appropriate level of classification and will be government-furnished equipment.

d. All users will complete the DoD Information Assurance Awareness training annually and will sign the Fort Hood Computer User Agreement.

e. All privileged users will be trained and certified in accordance with DoD 8570.01 and Army Best Business Practices.

f. All incidents, or suspected incidents, related to computer security will be reported through the unit IASO to the Fort Hood Information Assurance Manager.

g. Failure to follow any of the above procedures, proper security policies and regulations will result in immediate suspension of network access and privileges until compliance is confirmed.

h. Telephone and ILAN subscribers are responsible for the proper use of equipment. Under no circumstances will a subscriber move, alter, place an attachment on, or make any additions to official telephone or ILAN equipment, to include, but not limited to, hubs, routers, switches, and any multi-port devices.

i. The Network Enterprise Center will:

(1) Establish standardized patch management policies, procedures and tools.

(2) Maintain a network security webpage at http://www.hood.army.mil/doim; where the latest notices, patches, updates and service packs will be located for each access.

(3) Proactively monitor the network for new vulnerabilities and patches for all software and hardware identified on the network.

(4) Conduct risk assessments and report findings as required by regulation.

4. EXPIRATION. This Fort Hood Command Policy Memorandum supersedes the 14 October 2008 policy, DOIM-01, and will remain in effect until superseded or rescinded.

ROBERT W. CONE
Lieutenant General, USA
Commanding

DISTRIBUTION:
IAW FH Form 1853: A