



DEPARTMENT OF THE ARMY
Directorate of Army Information Management Support Center
2530 Crystal Drive,
Arlington, VA 22202-3944

REPLY TO
ATTENTION OF

AAIT-IM

17 November 2008

MEMORANDUM FOR: ALL IMCEN SUPPORTED ORGANIZATIONS AND USERS

SUBJECT: Acceptable Use of Government Furnished Equipment within the Headquarters Enterprise Network (HEN) or the Headquarters Classified Enterprise Network (HCEN)

1. References.

- a. AR 25-1, Information Management, 15 July 2005
 - b. AR 25-2, Information Assurance, 3 August 2007
 - c. AR 380-67, Department of the Army Personnel Security Program, 9 September 1988
 - d. The Department of Defense Directive (DoDD) 8500.1, "Information Assurance", 24 October 2002
 - e. The Department of Defense Instruction (DoDI) 8500.2, "Information Assurance Implementation", 6 February 2003
 - f. The Department of Defense Directive (DoDD) 8530.1, "Computer Network Defense" January 8, 2001
 - g. The Department of Defense Directive (DoDD) 8570.1 Information Assurance Training, Certification and Workforce Management, 15 August 2004
 - h. The Department of Defense Directive (DoDD) 8570.1-M, Information Assurance Workforce Improvement Program, 19 December 2005
 - i. Pacific LandWarNet Privileged User Acceptable Use Policy, Acceptance of Responsibilities, & Non-Disclosure Statement; HQ USARPAC, Fort Shafter, HI
- 2. Purpose.** To establish Information Management Support Center (IMCEN) directive on the proper use of government furnished equipment operating within the HEN or HCEN.
- 3. Scope:** This directive applies to all members of IMCEN and IMCEN supported agencies that use the HEN or HCEN to share Automated Information Systems (AIS) resources and process data.

AAIT-IM

SUBJECT: Acceptable Use of Government Furnished Equipment within the Headquarters Enterprise Network (HEN) or the Headquarters Classified Enterprise Network (HCEN)

4. Policy:

a) Automated Information Systems (AIS) are provided to personnel within Headquarters, Department of the Army and supported agencies to enhance job performance and communications.

b) All employees who must access government AIS for the performance of their assigned duties must have at least a favorable completed National Agency Check (with Inquiries for Government civilian employees). Waivers may be granted for limited access if the investigation paperwork has been submitted. This includes all temporary or seasonal hires.

c) Users requiring access to the HCEN are required to have a minimum of an interim secret clearance.

d) All users must receive initial security and information assurance training prior to being granted access to the government AIS. Each HQDA agency is responsible for information assurance and security training for their personnel. HQDA users will use <https://ia.gordon.army.mil/default.asp> as IA training courses websites.

e) Users will ensure that they lock their systems whenever they must leave their workstation for short periods of time during the duty day. All workstations should be configured to automatically lock after not more than 15 minutes of non-use or inactivity.

f) Users will restart their systems at the end of the day or whenever they are going to be away for an extended period of time. Systems should be left powered on to enable automatic, off-hours updates of security patches, upgrades, etc.

g) Users must utilize government provided Automated Information Systems (AIS) resources in a responsible manner and not engage in improper use of those resources. Information contained in the computers files is to be accessed or used for authorized business only. The content of any information made available to others via the network is the sole responsibility of the person who created the information. It is the user's responsibility to be aware of all applicable Federal laws, and Department of Defense (DoD), Army and agency regulations and policies governing the use of AIS and safeguarding information. The user will be liable for any violations of governing laws, regulations or policies

AAIT-IM

SUBJECT: Acceptable Use of Government Furnished Equipment within the Headquarters Enterprise Network (HEN) or the Headquarters Classified Enterprise Network (HCEN)

h) Users may never use computer systems, including email services, to:

(1) Establish commercial activities or for personal profit or gain.

(2) View, receive or transmit racially or ethnically offensive material.

(3) Harass, which includes: bullying, threats, statements of intimidation, derogatory comments, statements or messages relating to a person's religion, race, ethnic origin, gender, age, sexual orientation, marital status, veteran status of disability or any material which may be deemed offensive in nature that is not directly related to the individual's performance of duty.

(4) Post religious or political solicitations.

(5) Access of share agency proprietary/restricted, DoD Classified, For Official use Only (FOUO) or information protected under privacy statutes without authorization.

(6) Attempt to 'hack' the network or connected AISs, subvert data protection schemes, gain access, share or elevate permissions to data or AISs for which the user is not authorized.

(7) Internally test the security features of the AIS without authorization.

(8) Gain or attempt to gain unauthorized access to remote computers.

(9) Unauthorized entry, use, transfer, and tampering with the accounts and files others, interference with the work of others, and other computing facilities.

(10) Broadcast unsubstantiated virus warnings from sources other than system administrators or information assurance personnel.

(11) Publicizing unauthorized activities such as charity solicitations, unless otherwise permitted by law (e.g., Combined Federal Campaign (CFC) and Army Emergency Relief (AER) campaigns).

AAIT-IM

SUBJECT: Acceptable Use of Government Furnished Equipment within the Headquarters Enterprise Network (HEN) or the Headquarters Classified Enterprise Network (HCEN)

(12) Deliberately perform an act that will seriously impair the operations of the AIS.

(13) Deliberately misrepresent themselves or their data on the network.

(14) Engage in any activity that violates federal, state, or local laws with respect to intellectual property rights, the terms of software license agreements or other policies pertaining to computer software.

(15) Download from the Internet or cause to be loaded onto a government system, any files that are subject to copyright protection and to which the U.S. Government does not have license. This includes files containing music and/or movie videos.

(16) Send or receive chain letters.

(17) Access the Internet to participate in chat rooms, on-line games, personal accounts or other non-business related activities.

(18) Any other use that would reflect adversely on DoD or which is incompatible with public service (e.g., sending threatening or harassing electronic messages; accessing, storing, processing, displaying, or distributing offensive, obscene, or sexually explicit e-mail or pornographic images, virtual computer generated, or otherwise pornographic images and hate literature; unauthorized fundraising, gambling or similar activities; terrorist activities; partisan political activity, political activity, political or religious lobbying or advocacy), or any other use which violates statute or regulations is never authorized.

(19) Only IMCEN approved software will be loaded on Government Furnished Equipment (GFE). To receive approval for software, the IMCEN procedures must be followed. Users are not authorized to install software on the workstations or laptop computer. Users who violate this directive are subject to having their system access rights suspended or revoked pending the outcome of an investigation.

(20) Users are not authorized to place or cause to be placed any information on their workstations or network drives that is of a higher classification than that for which the workstation or network is accredited. In addition, users are not authorized to change the security settings on the government systems provided for their use. Changing basic input/output system (BIOS) settings and/or BIOS password is/are specifically prohibited.

AAIT-IM

SUBJECT: Acceptable Use of Government Furnished Equipment within the Headquarters Enterprise Network (HEN) or the Headquarters Classified Enterprise Network (HCEN)

(21) Users will protect and label all output generated under their accounts to include printed material, magnetic tapes, external media, system disks, and downloaded files.

(22) Users understand that all information processed on AISs is subject to monitoring. This includes e-mail and web browsing.

(23) Users are provided access to email, the Internet for personal use in accordance with acceptable use policies of Department of Defense (DoD), the Army and this document.

i. Violations of the above memorandum will result in the following:

1) Pursuant to referenced above violations of this policy by uniformed members of the armed forces may result in prosecution under the United States Code of Military Justice (UCMJ). Civilian employees who violate this policy may also be subject to adverse action or discipline in accordance with applicable laws and regulations.

2) If the violation is found to be criminal in nature, the Criminal Investigation Division will assume responsibility for the case.

3) If the violation is not criminal in nature but due to willful disregard by the user of this memorandum outlined in the DoD and ARs, the users access privileges will be revoked.

j. Organizations that become new members of the HEN and or HCEN will follow the IMCEN SOP.

k. Information Management Officers (IMOs) shall ensure that all users have read and understand this directive prior to being granted user login credentials to either the HEN or the HCEN. Each organization IMO shall ensure that this directive is reviewed annually by all federal and contractor employees. The IMO shall notify, in writing, IMCEN Information Assurance (IA), that an annual refresher briefing or review has been accomplished.

AAIT-IM

SUBJECT: Acceptable Use of Government Furnished Equipment within the Headquarters Enterprise Network (HEN) or the Headquarters Classified Enterprise Network (HCEN)

- 5. Point of Contact.** Ms. Emyrose Calicdan, IMCEN Information Assurance Division, 703-602-7394, Emyrose.calicdan@us.army.mil

Gabriele Daniel

GABRIELE DANIEL
Director, Information Management Support
Center

Glossary

ACIT	Assistant Chief of Information Technology
ADA	American Disability Act
AR	Army Regulation
CUI	Controlled Unclassified Information
CCC	Configuration Control Committee
CCE	Center of Contracting Excellence
CDR	Call Detail Record
CIOG6	Deputy Chief of Staff for Command, Control, Communications & Computers
CL	Customer Liaison
CMI	Classified Message Incident
COR	Contracting Officer Representative
CRF	Code of Federal Regulations
CSD	Customer Support Division
DA	Department of Army
DAA	Designated Approval Authority
DITSCAP	DoD Information Technology System Certification and Accreditation Program
DISA	Defense Information System Agency
DoD	Department of Defense
ESD	Enterprise Services Division
ESS-P	Enterprise Security Services-Pentagon
FOUO	For Official Use Only
FTS-2001	Federal Telecommunications Systems-2001
GFE	Government Furnished Equipment
HCEN	HQDA Classified Enterprise Network
HEN	HQDA Enterprise Network
HQDA	Headquarters Department of the Army
HQDA/IMCEN	Headquarters Department of the Army Information Management Support Center
IA	Information Assurance
IAD	Information Assurance Division
IAM	Information Assurance Manager
IASO	Information Assurance Security Officer
IAW	In Accordance With
IEEE	Institute of Electrical and Electronics Engineers
ICW	In Coordination With
IMCEN	Information Management Support Center
IMO	Information Management Officer
ISB	Installation Services Branch
ISP	Internet Service Provider
IT	Information Technology
ITMRA	Information Technology Management Reform Act (Clinger-Cohen Act)
JER	Joint Ethics Regulations
LAN	Local Area Network
MSN	Microsoft Network
NCR	National Capital Region
NISO	Network Infrastructure Services Organization
NSA	National Security Agency
OIP	Organization Inspection Program
OMB	Office of Management and Budget
ONS	Operational Needs Statement
OPM	Office of Personnel Management
PDA	Personal Digital assistants
PED	Wireless Portable Electronic Devices
PL	Public Law
POC	Point Of Contact
RAD	Requirements Analysis Division

SOP	Standard Operating Procedures
ST	Support Team
TSCO	Telephone Services Control Officer
WAN	Wide Area Network

IMCEN
Acceptable Use Policy Acknowledgement

I have read/been briefed on the IMCEN Acceptable Use of Government Furnished Equipment within the Headquarters Enterprise Network (HEN) or the Headquarters Classified Enterprise Network (HCEN). I understand that the government system provided me for use in the accomplishing my mission belongs to the government and I will take no actions to abuse the privilege I am being granted as a user on the HEN/HCEN. I understand that if I violate the provisions of this policy I may have my network access privileges terminated placing my ability to perform my assigned duties in jeopardy.

Agency (Please Print)

Date

Last Name, First, MI

Rank/Grade

Signature

Phone Number