DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
2250 STANLEY ROAD
FORT SAM HOUSTON, TEXAS 78234-6100

REPLY TO ATTENTION OF

MCCS-BIM

24 FEB 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management Policy 25-03, User Responsibilities for Information Systems Sustainment

1. REFERENCES.

a. DOD Directive 5500.7-R, Joint Ethics Regulation (JER), thru Change 4, 6 August 1998.

b. AR 380-19, Information Systems Security, 27 February 1998.

c. AR 25-1, Army Information Management, 31 May 2002.

d. The FSH Regulation 690-26, Conduct and Discipline, 5 March 1997.

e. Memorandum, MCCS-Z, 7 January 2002, subject: User Responsibilities for Information Systems Sustainment Policy.

f. The USAG FSH Policy Statement Number 31, subject: Use of Federal Government Communications Systems and Resources, 1 July 2002.

2. PURPOSE. This policy outlines the responsibilities of the information system user on Fort Sam Houston (FSH), satellite sub-installations, and all other work sites connected to the installation network. This policy assigns responsibilities, and provides guidance in applying information technology best business practices in day-to-day use and protection of information systems.

3. SCOPE. This policy applies to all organizations receiving reimbursable services from the Information Technology Business Center (ITBC) to the extent of the products and services they use.

4. POLICY. Each of the following policy categories has several components of which users have some level of accountability.

a. Requirements. Each user organization is responsible for identifying its own functional common-user Information Management/Information Technology (IM/IT) business requirements to the Business Development Office for incorporation in the appropriate Installation Support

Agreement. Each user organization must submit project or unique requirements to the ITBC Director, ATTN: MCCS-BIM-B (Business Systems Solutions Division). All IM/IT technical solutions must meet DOD, DA, HA/MEDCOM, and installation standards, or a waiver will be necessary. User organizations will forward waiver requests to the ITBC Director, ATTN: MCCS-BIM (Architect).

b. User Training. It is the obligation of the user to request supervisor approval to attend training classes, seminars, educational assistance programs, etc., in order to increase their level of proficiency.

c. User Assistance. Users will call the ITBC Help Desk (221-HELP) for IT assistance. Supervisors will discourage alternative, unofficial desktop support from non-ITBC personnel.

d. Equipment.

(1) Users, or unit/activity designated point of contact (POC), will identify all IT installation, move, add, and change (IMAC) requirements to ITBC. The IMACs of government equipment and equipment on lease will be done by ITBC to ensure correct technical configuration and asset management accuracy. Users or POCs will provide sufficient notification (at least 10 work days) to ITBC in order to meet date, time, and location requirements.

(2) User, or unit POC, will identify their functional requirements to ITBC for new leases, refresh of expiring leases, and new equipment purchases. Maximum lead-time (60-90 calendar days) will ensure ITBC meets customer requirements.

(3) Users are held accountable for the integrity, care, and property accountability of all IT equipment, both government-owned and leased.

(4) User or POC will coordinate final disposal of IT equipment with ITBC.

e. Users or POC will request network accounts from the ITBC Director, ATTN: MCCS-BIM-S (Security Division).

f. Each user is responsible for utilizing the computing equipment and network in accordance with the banner display at network or application logon, which is based upon higher headquarters' policy and the DOD Joint Ethics Regulation. (Reference 1a).

g. Infostructure resources:

(1) Users will only consume network file space and/or bandwidth for official government business, except as defined in reference 1f.

(2) Users will not abuse the functionality of the Internet for non-business use (i.e., music videos, etc.).

(3) Users will not use government equipment to access material that is sexually oriented, demeans others, or that is of an extremist or terrorist nature (Reference 1e).

(4) Users will not abuse Email privileges. Users will perform regular housekeeping by purging or otherwise cleaning their Email accounts. Users will not send chain letters, jokes, pornography, daily quotes, or unsubstantiated virus warnings in or attached to Email notes over the installation network.

(5) Users will immediately report suspected viruses to ITBC, ATTN: MCCS-BIM-S (Security Division).

(6) Users will not use telecommunication services (telephones, cellular phones, pagers, radios, fax devices, etc.) for unofficial purposes except as noted in Reference 1f.

(7) Incoming collect calls to official work sites are not permissible except in cases where ITBC grants an exception for operational requirements.

(8) Personal long distance calls may be made from official work sites, if the user has first obtained the permission of his/her supervisor and the call is made at no expense to the Government. Government calling cards may <u>only</u> be used for official business.

(9) All tenant organizations will be responsible for respective costs of all telecommunications services incurred using telephone equipment, data circuits, calling cards, cellular phones, pagers, or other special communications devices.

5. This policy will be reviewed 2 years from the implementation date.

6. The point of contact is Ms. Cynthia S. Helton, Director, ITBC, 221-5281, or email address Cynthia.helton@samhouston.army.mil.

DANIEL F. PERUGINI
Brigadier General, MC
Commanding

DISTRIBUTION:
A, B, Plus:
30 – MCCS-BHR-AS, Plus:
All Garrison Activities