

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400
APO AE 09131

STAFF MEMORANDUM
NUMBER 100-3

1 July 2002

COMMAND, CONTROL AND COMMUNICATIONS

Internet Access and Use of Government Information Systems and Software

1. **Summary.** To provide guidelines governing personal use of computer networks at Headquarters, United States European Command (HQ USEUCOM).
2. **Applicability.** This policy applies to users of HQ USEUCOM computer networks and systems.
3. **Internal Controls.** This Staff Memorandum contains internal control provisions and is subject to the requirements of the internal management control program. The applicable internal control directive is ED 50-8, Internal Management Control Program.
4. **Suggested Improvements.** ECJ6 Headquarters Support Division is responsible for this publication. If you have suggestions for improvement, or if you find errors, please contact us at:

HQ USEUCOM, ECJ6-H
Unit 30400
APO AE 09131

5. **References.**
 - a. Public Law 100-235, The Computer Security Act of 1987.
 - b. Department of Defense (DoD) 5500.7-R, Joint Ethics Regulation (JER), 30 August 1993.
 - c. EUCOM Directive (ED) 25-5, Security Information Assurance Policy, 10 March 1999.

This staff memorandum supersedes SM 100-3, dated 5 May 1997.

6. **Background.**

a. The Internet is a fundamental communications tool providing the widest practicable and appropriate use of information. The Internet is also recognized as a worldwide electronic access mechanism to information and services. HQ USEUCOM promotes the widest permissible use of government information systems to access and exchange information in an automated environment. This includes, but is not limited to, accessing the INTERNET, browsing the World Wide Web (WWW), and communicating via electronic mail.

b. This memorandum defines policy and gives specific examples of what is permissible and what is not when dealing with personal use of government computer networks and the Internet.

7. **Policy.**

a. Staff members are encouraged to use their government computers to access the WWW and develop their information skills, consistent with legal and ethical rules.

b. Restrictions. Your authorization to use government computer networks is subject to the following restrictions and constraints:

(1) Does not adversely affect the performance of your official duties;

(2) Is of reasonable duration and frequency, and whenever possible, made during your personal time, such as after duty hours or during lunch periods;

(3) Serves a legitimate public interest, such as keeping employees at their desks rather than requiring the use of commercial systems; educating the employee on the use of the communications systems; enhancing the professional skills of the employee;

(4) Does not overburden the communications systems, such as downloading large or complex graphics, sending broadcasts or group mailings, or other high bandwidth operations;

(5) Does not create any significant additional cost to the Staff or the DoD;

(6) Does not result in significant use of consumable resources (e.g., printer paper and toner);

(7) Does not incur any tolls, charges, or other fees for which the government is liable, except when specifically authorized in writing at the directorate level; and

(8) Does not reflect adversely on HQ USEUCOM, the Department of Defense, or the United States Government and shall not violate statutes or regulations, specifically including DoD Instruction 5500.7R (Joint Ethics Regulation).

(9) Examples of adverse use include:

(a) Viewing/transmitting/receiving pornographic or obscene material;

- (b) Introducing classified information into an unclassified system or environment;
- (c) Storing, accessing, processing, or distributing classified, proprietary, sensitive, or "For Official Use Only" (FOUO) information on a computer or network in violation of established policies;
- (d) Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement;
- (e) Writing, coding, compiling, storing, deliberately transmitting, or transferring malicious software code, to include so-called viruses, logic bombs, worms, and macro viruses;
- (f) Partisan political activity, political or religious lobbying, advocacy of activities on behalf of organizations having no affiliation with the federal government, or dissemination of religious materials outside an authorized command religious program;
- (g) Activities whose purposes are for personal or commercial financial gain, including advertising or solicitation of services, stock trading, or sale of personal property, with the exception of using a command approved mechanism such as a welfare and recreation electronic bulletin board for advertising personal items for sale;
- (h) Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g., welfare and recreation car washes);
- (i) Gambling, wagering, placing of any bets;
- (j) Illegal, fraudulent, deceptive, malicious, or criminal activities;
- (k) Posting personal home pages on government computer servers; or
- (l) Other uses incompatible with public service, including activities which present a conflict with government interests, activities which compromise federal government systems, activities in violation of DODINST 5500.7R.

c. Electronic Mail Policy.

- (1) Whenever you send electronic mail, your name and UserID are included in each mail message. You are responsible for all electronic mail originating from your UserID.
- (2) The following actions are prohibited:
 - (a) Sending e-mail that is racist, promotes hate crimes, or is subversive in nature is prohibited;
 - (b) Forgery (or attempted forgery) of electronic mail messages;
 - (c) Attempts to read, delete, copy, or modify the electronic mail of other users;

(d) Sending or attempting to send harassing, obscene, and/or other threatening email to other users;

(e) Attempts at sending unsolicited junk mail; "for-profit" messages or chain letters;
or

(f) Automatically or manually forwarding government e-mail to commercial internet service provider (ISP) accounts so that work can be done at home.

(g) Use of Web-Based or Internet Service Provider (ISP) E-Mail Accounts for Official Business. HQ USEUCOM personnel will employ government-owned e-mail systems for authorized, unclassified U.S. government business. HQ USEUCOM personnel will not use unapproved accounts (such as HOTMAIL or YAHOO MAIL) for official business unless specifically authorized to do so by the ISSO.

d. Unauthorized Software. HQ USEUCOM computer systems are accredited to use specific software, which was tested and evaluated. Any user introduction of software not part of the original configuration is unauthorized software. This policy is intended to minimize the risk of introducing malicious software, i.e., a virus, into a system. Adherence to the provisions of this policy will decrease the vulnerability of our systems. Prohibited software includes:

(1) Games;

(2) Public domain software or shareware, which have been obtained from unofficial channels;

(3) All software applications which have been developed outside government-approved facilities, such as those developed on personally owned computers at home or software acquired via non-Government "bulletin boards." Personally owned software (either purchased or gratuitously acquired). Software purchased using employee funds (from an activity such as a coffee fund);

(4) Unknown source software;

(5) Illegally (pirated) copied software in violation of copyright rules; and

(6) Music and video or multimedia compact disks not procured through official Government channels. Non-government CD's may have hidden boot records or viruses, therefore they are not allowed in any government computer.

8. **Consent to Monitoring.** Your use of government computer networks and systems is monitored. Activity on computer networks, government or otherwise, is not anonymous and does not provide any expectation of privacy.

9. **Policy Violations.** This staff memorandum is directive in nature. Failure to comply with provisions of the Joint Ethics Regulation, as incorporated into this staff memorandum, may result in revocation or suspension of computer system accounts, loss of access to all HQ USEUCOM

1 July 2002

SM 100-3

automated information systems, punishment under the Uniform Code of Military Justice, termination of employment, and/or criminal prosecution. Report violations to the Information System Security Officer (ISSO) for the system in question via the HQ USEUCOM C4I Helpdesk at 430-4174, or the HQ USEUCOM JDISS-CSE Helpdesk at 430-4272 for Intel systems.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

DANIEL J. PETROSKY
Lieutenant General, USA
Chief of Staff

AVA N. WEBB-SHARPLESS
Lt Col, USAF
Adjutant General