

DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY FIELD ARTILLERY CENTER AND FORT SILL
FORT SILL, OKLAHOMA 73503

USAFACFS Regulation
No. 380-1

2 April 2001

Security
INTERNET SECURITY

Supplementation of this regulation is prohibited
unless specifically approved by HQ, USAFACFS

- 1. PURPOSE.** This is a joint regulation between the Security Division, DPTM and DOIM. This regulation provides minimum guidelines for access and use of the Internet from Fort Sill computer systems. It establishes safeguards to detect and prevent technical attacks made on Fort Sill systems and ensures classified, sensitive but unclassified, For Official Use Only, or Privacy Act information is not released to unauthorized personnel. Commanders or activity chiefs may impose more stringent procedures provided there is prior coordination with Security Division, DPTM.
- 2. SCOPE.** This regulation applies to all military, civilian, and contract personnel operating on Fort Sill or Fort Sill-controlled sites. Except as stated in paragraph 8, Home Pages, this regulation does not apply to personal electronic mail (E-mail) accounts or subscriptions to computer services that personnel use for nongovernment business from a nongovernment affiliated system.
- 3. POLICY.** Many unclassified computer systems on Fort Sill allow users to access the Internet (including E-mail, browsers, dial-up, etc.). Fort Sill promotes the use of the Internet to achieve installation goals. Individuals must use the same discretion and courtesy in their electronic communications that they would in any other official interaction.
- 4. CLASSIFIED AND SENSITIVE BUT UNCLASSIFIED INFORMATION.** Do not connect systems processing or containing classified information to the Internet without prior written approval from Security Division, DPTM. Sensitive but unclassified information is releasable only with prior approval by the Release Authority as detailed in AR 360-5. Systems with Internet connectivity that process sensitive but unclassified information must be identified as such in accreditation documentation.

This regulation supersedes USAFACFS Regulation 380-1, 24 February 1998.

5. OPERATIONAL SECURITY. Internet sites and message traffic are lucrative intelligence sources targeted by many activities for information collection. Users will not leave a system password-enabled if they are not physically present to ensure protection of the information accessible by the system. Users should report suspicious activity to their organization's Information Systems Security Officer (ISSO). Suspicious activity may include obvious tampering or theft. Any user aware of improper activity to include a violation of this regulation is responsible for reporting that information to Security Division, DPTM.

6. INTERNET ACCESS.

a. An account is any established routine path of access to services or information through the Internet that is associated with a user login name to identify the user and associate the user with privileges on that account. Accounts will have identified users who will be assigned passwords.

b. A password is a unique identifier (usually randomly generated) assigned to an account. The password authenticates the user's identity and permits use of the account. Passwords will not be installed so as to automatically engage; they must be manually keyed in at each entry to the systems. Users will not share or disclose those passwords with unauthorized personnel. Users will not install password programs on systems without prior coordination with their ISSO including providing all systems passwords to the ISSO. ISSOs will maintain documentation of all passwords in their organization. ISSOs will disclose passwords only in the event of an emergency request by their commander or director. The ISSO will prepare a memorandum of record documenting the request and within 24 hours will submit a request to the Director of Information Management (DOIM) for change of passwords.

c. Users will protect passwords at the same sensitivity level as the information they are accessing and as a minimum will manage them as sensitive but unclassified, nonreleasable information. Users will immediately report compromise or suspected compromise of passwords to their ISSO. Reporting must never be delayed more than 24 hours after the compromise or suspected compromise. ISSOs will report such information to Security Division, DPTM, on the same day the information is received.

7. INTERNET USE.

a. Users will use their accounts for authorized U.S. government purposes only. Such use may include keeping current with professional information of a field, acquiring publicly-available information of value to the organization, conducting unclassified contract/COTR-related business, and keeping current with unclassified office matters while away from the workplace.

b. Users will not attempt to “talk around” classified topics while communicating electronically. Classified discussions will not take place on automated systems (such as E-mail or newsgroup discussions) without written approval from Security Division, DPTM.

c. Users are authorized to upload and download programs and files via the Internet from an unclassified system provided a current virus scan program is installed, configured and in use to detect viruses upon receipt of infected files. Antivirus programs must be approved by Security Division, DPTM, and recorded on accreditation documentation. Users may download items for official government business only and must follow the release authority guidance in paragraph 4 of this regulation to upload information.

d. Users may not use their official accounts for purposes including pornography, chain letters, unofficial advertising, soliciting or selling, or any other activity that would bring personal profit or gain, or would discredit the Department of Defense, the United States Army or Fort Sill. The Joint Ethics Regulation and TRADOC Regulation 25-70 allow supervisors who are commissioned officers or civilians in the grade of GS-11 or higher to authorize limited nonofficial use of the Internet accounts if such use does not interfere with mission accomplishment and is of reasonable duration and frequency. Commander, USAFACFS, has determined permissible nonofficial uses of the Internet by Fort Sill personnel in USAFACFS Memorandum 25-10. Consult the memorandum for more detailed guidance. Normally, such authorized use should be limited to an employee’s own time, such as during breaks and before or after duty hours.

e. Holders of official accounts will be required to sign FS Form 116 (User’s Agreement for Account Access). These forms are available from unit/activity ISSOs. ISSOs will maintain originally signed forms for all unit/activity account holders.

f. In cases where groups of computers are provided (i.e., for educational purposes) the ISSO or TASO is required to maintain accountability of access to systems so as to determine individual activities on computer systems. For example, a user would sign into a log for a particular system with a time notation for the beginning and ending time of use. In no case will a user access a group of computers or a network that exceeds their clearance, access level, or need-to-know.

8. HOME PAGES. Home pages related to Fort Sill-affiliated units or activities will be protected through access controls established in USAFACFS Regulation 25-10. Personal home pages of employees affiliated with Fort Sill will not contain information that requires release as detailed in AR 360-5 unless prior approval has been received by the appropriate release authority. Authors of personal home pages will not include information that is Classified, For Official Use Only, or extracted from Privacy Act records. Suspected violations will be referred to Security Division, DPTM.

9. LEGAL RESTRICTIONS ON INTERNET USE. Internet use by Federal employees (military, civilian, DOD-contractors) is subject to the same laws, regulations, and

procedures governing unclassified telephone calls or participation at professional conferences. These include regulations governing contacts with foreign nationals, as well as contacts with the media and Congress. Users must comply with the Copyright Act, the Freedom of Information Act, and the Privacy Act.

a. Copyright, Title 17, U.S.C. The copyright laws of the United States provide that the owner of copyright (usually the originator of the work) has exclusive rights to reproduce, distribute, prepare derivative works, and publicly display or perform a work. Users will respect the legal protection provided by copyright, license, and authorship of messages, programs, data, and, programs language.

(1) Unless there is a specific notice to the contrary, material on the Internet is protected by copyright even if it does not have a copyright notice (such as the “c” in a circle or the word “copyright” followed by a name and date).

(2) There is a limited exception to the copyright statute known as the “fair use” exception. Under this rule, it is fair to use a copyrighted work without the owner’s consent under very limited circumstances. Determinations on such factors will not be made by individual users on Fort Sill. Requests for consideration and additional guidance will be submitted to Administrative Law Division, Staff Judge Advocate.

(3) Users will not download, upload, or use unlicensed programs or copyrighted material without the express consent of the owner of such material. Users will be held personally accountable for such activity and violations will be reported by Security Division, DPTM, to the appropriate law enforcement activity.

b. Privacy Act (5 U.S.C. PARA 552a). The Privacy Act, like the copyright laws, applies equally to electronic data. The Privacy Act is one of the laws governing the Army’s collection and dissemination of information about U.S. citizens and permanent resident aliens. If such information can be retrieved from a system of records by name of individual or by some other identifying particular (such as social security number), it is a Privacy Act record. Because of the Privacy Act restrictions, users may not post or send in any manner Privacy Act records outside Army control without guidance from the Administrative Law Division, Staff Judge Advocate.

c. Collection, Retention, and Dissemination of Information; Contacts with U.S. Persons (Executive Order 12333). EO 12333 governs the Army’s interactions with U.S. persons and the collection, retention, and dissemination of information concerning U.S. persons. Users may not solicit or gather information on the domestic activities of U.S. persons through the Internet.

d. Interception of Communications (Fourth Amendment, Electronic Communications Privacy Act, and Executive Order 12333). In the United States, users may not intercept the private transmissions of other users or attempt to access stored electronic communication of others without authorization. Users may, however, access electronic

bulletin boards, list servers, and discussion groups that are generally accessible to any member of the public provided that the activity complies with this regulation.

10. CONTACTS WITH THE MEDIA AND CONGRESS. All contacts with the media concerning Fort Sill matters must be made through Fort Sill Public Affairs Office. Fort Sill Adjutant General's office coordinates all Congressional inquiries.

11. CONTRIBUTING TO THE INTERNET. Users of official accounts may participate in E-mail correspondence and contribute to its publicly accessible services. They may not, however, release official Army information. Only the Public Affairs Office may authorize release of information identified as Fort Sill's official position. When contributing to discussions from a Fort Sill affiliated computer system on publicly accessed Internet services and sites or throughout E-mail correspondence, users must provide a disclaimer that their views do not represent an official Army or Fort Sill position. Users and their comments may be identified with the Army, the communications may be widely distributed, and hostile intelligence services may be tracking communications traffic originating from official accounts. For these reasons, users should exercise caution in their posting and correspondence.

12. RECORDKEEPING. Electronic communication may be considered Federal records. Those that qualify as records must be managed according to their information content. Therefore, users must follow AR 25-11 and AR 25-400-2 with respect to such records. Assistance will be provided by the Installation Administrative Support Team, Directorate of Information Management.

13. AUDITS. Activities occurring on automated systems are subject to audit. Electronically stored audit records, including activity reports and E-mail files, can be traced to the account holder. Such records may be used to support claims of violations of Army regulations, federal law, and other civil statutes. The Information Systems Security Manager will coordinate any search or review of holdings of electronic data for purposes of responding to requests for information pursuant to Freedom of Information Act, Privacy Act, Congressional, or any other investigative inquiry.

14. COMPLIANCE. Individual users are responsible for their action on their accounts. Paragraphs 4, 5, 6, 7, 8, and 10 of this regulation are punitive. Violators of these paragraphs are subject to punishment under UCMJ, federal personnel laws, or federal and state statutes where they apply. Security Division, DPTM, will immediately notify the appropriate system administrator to withdraw all Internet access to those users violating paragraphs 4, 5, 6, 7, 8, or 10 and will then determine suitability for reissuance of access.

(ATZR-TC)

FOR THE COMMANDER:



ROBERT A. CLINE
COL, FA
Chief of Staff

PHYLLIS R. BACON
Director of Information
Management

DISTRIBUTION:
Fort Sill Internet