

Headquarters
US Army Garrison Command
Fort Knox, Kentucky 40121-5717
7 January 2008

*Fort Knox Reg 25-70

Information Management

PROCEDURES FOR THE ENTRY OF INFORMATION INTO THE FORT KNOX WORLD WIDE WEB (WWW) AND ARMY KNOWLEDGE ONLINE (AKO) WEBSITES AND USE OF FORT KNOX COMMUNICATION RESOURCES

Summary. This regulation provides guidance and procedures for entry of information into the Fort Knox WWW/AKO websites and use of Fort Knox communications resources.

Applicability. This regulation applies to all Fort Knox major activities, directorates, and staff offices/departments and Partners in Excellence.

Suggested Improvements. The proponent of this regulation is Directorate of Information Management. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Directorate of Information Management (IMSE-KNX-IMA), Fort Knox, KY 40121-5717.

1. References.

- a. AR 25-1, Army Knowledge Management and Information Technology, 15 July 2005.
- b. TRADOC Regulation 25-1, Information Resource Management, 16 September 2006.
- c. AR 25-2, Information Assurance, 24 October 2007.

2. Due to security and legal ramifications, careful consideration must be given before entering any information into the Fort Knox WWW/AKO websites. Appendix A of this regulation provides guidance and procedures for entry of information into the Fort Knox WWW/AKO websites and outlines the different categories of information and their releasability into the Fort Knox WWW/AKO websites.

3. The Internet provides a tremendous resource of information exchange and other communications through vehicles such as mail list servers, data bases, files, and websites. Appendix D of this regulation contains guidance on use of Fort Knox communication resources used to access this information. These resources include, but are not limited to the following: Government-owned personal computers, networks, routers, gateways, modems, telephone lines, and software. This policy must be adhered to in order to prevent misuse of these resources.

*This regulations supersedes Fort Knox Reg 25-70, 12 April 2000.

4. The Fort Knox WWW/AKO are the only websites for The US Army Armor Center and Fort Knox. Subordinate organizations and activities will not create their own WWW Internet websites; however subordinate organizations and activities may be allowed their own AKO organizational site after coordination with the Fort Knox Webmaster. Before placing information on the Fort Knox WWW/AKO websites, coordination must be made with the Fort Knox Webmaster; Security Division, Directorate of Plans, Training, Mobilization, and Security; Public Affairs Office; and Staff Judge Advocate. Format for the approval document is located at Appendix B of this regulation. After approval from the three agencies above, the Fort Knox Webmaster will place this information on the WWW website. Updates and simple corrections may be coordinated with the Fort Knox Webmaster; however, all major changes to previously approved content must also follow this approval process. Graphical enhancements, typographical corrections, and original design will be coordinated with the Fort Knox Webmaster, phone 4-7122.

MARK D. NEEDHAM
COL, AR
Commanding



ROBERT L. BROOKS
Director, Information Management

DISTRIBUTION:
A

Appendix A
Releasability Guide for the Fort Knox World Wide Web Site

A-1. Information contained on the Fort Knox WWW website is subject to the policies and clearance procedures prescribed in AR 360-1, chapter 5, for release of information to the public. In addition, Fort Knox organizations will not make the following types of information available on the Fort Knox WWW website:

- a. Classified and restricted or limited distribution information.
- b. For Official Use Only (FOUO) information.
- c. Unclassified information that requires special handling (for example, Encrypt For Transmission Only, Limited Distribution, and scientific and technical information protected under the Technology Transfer Laws).
- d. Sensitive information such as proprietary information, pre-decisional documents, and information that must be protected under legal conditions such as the Privacy Act.
- e. Freedom of Information Act-exempt information. Lists of names and other personally identifiable information of personnel assigned within a particular component, unit, organization, or office are prohibited on the Fort Knox WWW website. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties—such as battalion and higher commanders and command sergeants major, PAOs, or other personnel designated as official command spokespersons—is permitted.
- f. Documents or information protected by a copyright.

A-2. **Classified Military Information (CMI).** (Reference AR 380-5, 29 September 2000, Department of the Army Information Security Program.) This information is not releasable for placement on the Fort Knox WWW website or the Internet under any circumstances. CMI is sensitive information that requires special protection. According to its degree of sensitivity, CMI is identified by a level of security classification: CONFIDENTIAL, SECRET, or TOP SECRET. The CMI information will never be placed on the Fort Knox WWW or AKO websites. Transmission of CMI will only be accomplished on an accredited system protected by an approved encryption product.

A-3. **Controlled Unclassified Information.** This information is not releasable for placement on the Fort Knox WWW website. FOUO and below may be allowed on the Fort Knox AKO website only after coordination with the Fort Knox Webmaster and appropriate AKO accessibility restrictions have been implemented.

(This page intentionally left blank)

Appendix B

Sample Request for Entry of Information into the Fort Knox World Wide Web (WWW) Website

LETTERHEAD IF REQUIRED

(OFFICE SYMBOL)

(Date)

MEMORANDUM THRU

Public Affairs Office (IMSE-KNX-PA)

Directorate of Plans, Training, Mobilization, and Security (IMSE-KNX-PLS)

Installation Legal Office (IMSE-KNX-LA)

FOR Directorate of Information Management (IMSE-KNX-IMA/Webmaster)

SUBJECT: Request for Entry of Information into the Fort Knox World Wide Web (WWW) Website

1. Purpose. To submit the enclosed information for entry into the Fort Knox (WWW) website.

SUBJECT:

DATE:

DISTRIBUTION RESTRICTION STATEMENT (if applicable):

2. Recommendation. That the enclosed information be approved for entry into the Fort Knox (WWW) website.

3. Justification. (STATE JUSTIFICATION).

4. Point of contact is (NAME), phone (X-XXXX).

Encl(s)

(COMMANDER'S/DIRECTOR'S
SIGNATURE)

(This page intentionally left blank)

Appendix C

Official and Authorized Uses of Telecommunications and Computing Systems

C-1. The use of DOD and other government telephone systems, e-mails, and other systems (including the Internet) are limited to the conduct of official business or other authorized uses. Commanders and supervisors at all levels will make anyone using Government telecommunications systems aware of permissible and unauthorized uses. Local policies and procedures will be announced, as necessary, to avoid disruptions of telecommunications systems. The DODD 5500.7-R, Joint Ethics Regulation, Section 2-301, serves as the basis for Army policy on use of telecommunications and computing systems. Users will abide by these restrictions to prevent security compromises and avoid disruptions of Army communications systems.

C-2. All communications users must be aware of security issues and their consent to monitoring for all lawful purposes, of restrictions on transmitting classified information over unsecured communications systems, of prohibitions regarding release of access information such as passwords, and the need for care when transmitting other sensitive information.

C-3. Commanders will recover toll charges for unauthorized personal telephone calls placed on official telephones by personnel in their organizations. Personnel making unauthorized unofficial telephone calls may be subject to disciplinary action as well as charged for the calls.

C-4. Official business calls and e-mail messages are defined as those necessary in the interest of the Government (for example, calls and e-mail messages directly related to the conduct of DOD business or having an indirect impact on DOD's ability to conduct business).

C-5. Official use includes health, morale, and welfare (HMW) communications by military members and DOD employees who are deployed in remote or isolated locations for an extended period of time on official DOD business. The installation or theater commander will institute local procedures to authorize HMW communications when commercial service is unavailable, or so limited that it is considered unavailable. HMW calls may only be made during nonpeak, nonduty hours and must not exceed 15 minutes. Emergency calls may exceed this limit.

C-6. Authorized uses of communications systems. Authorized use includes brief communications made by DOD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DOD employee's usual work place that are most reasonably made while at the work place (such as checking in with spouse or minor children, scheduling doctor and auto or home repair appointments, brief Internet searches, and e-mailing directions to visiting relatives). Such communications may be permitted if they:

a. Do not adversely affect the performance of official duties by the employee or the employee's organization.

b. Are of reasonable duration and frequency, and whenever possible, are made during the employee's personal time (such as during lunch, break, and other off-duty-periods).

- c. Are not used for activities related to the operation of a personal business enterprise.
- d. Long distance (toll) calls, are:
 - (1) Charged to the employee's home phone number or other non-Government numbers (third party call).
 - (2) Made to a toll-free number.
 - (3) Charged to the called party of a non-Government number (collect call).
 - (4) Charged to a personal telephone credit card.
- e. Serve a legitimate public interest (such as keeping employees at their desks rather than requiring the use of commercial systems, educating DOD employees on the use of communications systems, improving the morale of employees stationed for extended periods away from home, enhancing the professional skills of DOD employees, and job-searching in response to Federal Government downsizing).

C-7. Other prohibitions on use of Army communications systems include the following:

- a. Use of communications systems in a way that would reflect adversely on DOD or the Army (such as involving pornography or access to pornography websites; chain e-mail messages; unofficial advertising, soliciting or selling via e-mail; and other uses that are not compatible with public service).
- b. Use of communications systems for unlawful activities, commercial purposes or in support of "for profit" activities, personal financial gain, personal use inconsistent with DOD policy, or uses that violate other Army policies or public laws. This may include, but is not limited to, violation of intellectual property, gambling, terrorist activities, and sexual or other forms of harassment.
- c. Political transmission, including transmission which advocates the election of particular candidates for public office.
- d. Misuse. Both law and Army policy prohibit, in general, the theft or other abuse of computing facilities. Such prohibitions apply to e-mail services and include, but are not limited to the following: unauthorized entry, use, transfer, and tampering with accounts and files of others; interference with the work of others; and interference with other computing facilities.
- e. Interference. Army communications systems will not be used for purposes that could reasonably be expected to cause, directly or indirectly, congestion, delay, or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with others' use of communications. Examples of interference include, but are not limited to:

- (1) Create, download, store, copy, transmit, or broadcast chain letters.
- (2) "Spam" exploits list servers or similar broadcast systems for purposes beyond the intended scope to amplify the widespread distribution of unsolicited e-mail.
- (3) Send a "letter bomb" that re-sends the same e-mail message repeatedly to one or more recipients, to interfere with the recipient's use of e-mail.
- (4) Broadcast unsubstantiated virus warnings from sources other than systems administrators.
- (5) Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting smaller populations.

C-8. Guidance for telephone calls while at a temporary duty location is reflected in the Joint Travel Regulations (JTR).

C-9. Abuse of DOD and Army telecommunications systems, to include telephone, e-mail systems, or the Internet, may result in disciplinary action.

(This page intentionally left blank)

Appendix D
Guidance on Use of Internet Resources

D-1. Reference. Department of Defense (DOD) 5500.7-R, Joint Ethics Regulation (JER), 30 August 1993 (w/ch2).

D-2. Use of Federal Internet resources “shall be for official use and authorized purposes only” (JER 2-301). “Authorized purposes” may include personal use as permitted by “Agency Designees” within specified parameters.

D-3. Policy is hereby established for personal use of Federal Government Internet resources by Fort Knox personnel. Supervisors may issue more restrictive guidance.

a. Permission to use computers to access and use Internet resources for professional development purposes, subject to ensuring that primary duties and mission are accomplished.

b. You also have permission to use your computers to access and use these Internet resources for any other personal reason, such as reading a business magazine or checking stock quotes, but you may do this only before and after work hours, during lunch periods, or during other authorized breaks during the work day. To ensure such use does not adversely affect the performance of official duties and serve a legitimate public interest, this permission is subject to the following:

(1) Whenever possible, access Internet resources before or after work hours or during lunch and other authorized breaks.

(2) If made during your normal work hours, keep the communications connections INFREQUENT and SHORT.

c. This permission does not extend to personal use to solicit business, advertise, or engage in other selling activities in support of private business enterprises, fundraising activities (other than those permitted by JER 3-210), or any other use that would reflect adversely on the Army or is incompatible with public service (e.g., chain letters, harassing e-mail, surfing sexually oriented sites, or downloading sexually oriented material).

D-4. In appropriate cases, your supervisor may also authorize you to use Internet access in support of your personal and private participation in non-Federal and not-for-profit professional organizations (see JER 3-305), subject to the limitations in paragraph D-3 above.

D-5. Be aware that any use of Government communication resources is with the understanding that such use is generally not secure, not anonymous, and serves as consent to monitoring.