

FORT KNOX COMPUTER-USER AGREEMENT

For use of this form, see AR 380-19

As a user of a Fort Knox Automated Information System (AIS), I will adhere to the following security rules:

1. I will use Army information systems (computers, systems, and networks) only for authorized purposes.
2. I will not install any software or hardware on any Government-owned computer (for example, client-workstation, server) without first getting written approval from my Information Assurance Security Officer (IASO). I also understand that shareware and freeware, such as Morpheus, ICQ, IMesh, Napster, etc. will not be installed on government-owned computers.
3. I will not try to access data or use operating systems or programs, except as specifically authorized.
4. I know I will be issued a user identifier and a password to authenticate myself on the Fort Knox network. After receiving them-
 - a. I will not allow anyone else to have or use my password. If I know that my password has been compromised, I will report to my IASO/IMO for a new one.
 - b. I am responsible for all activity that occurs on my individual account and the account is protected by a password that is known only by me.
 - c. I will ensure that my password is changed at least every 3 months or when compromised.
 - d. I understand that if my password does not meet current FORT KNOX policy (8-14 characters, alpha-numeric, at least 1 alpha in caps, and 2 numeric), I will not be authenticated on the network. I also understand that the first 5 characters of my password may not be duplicated until 5 password changes have occurred.
 - e. I will not store my password on any processor or microcomputer or on any magnetic or electronic media unless approved in writing by the IASO/IMO.
 - f. I will not tamper with my computer to avoid adhering to FORT KNOX password policy.
 - g. I will not leave my computer unattended while logged on or I will secure my computer with the lock computer utility.
5. I know that it is a security violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.
 - a. I will not access or try to access information or accounts without proper authorization through the appropriate channels.

b. I will not enter information into a system if the information has a higher classification than that for which the system is rated. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the IASO.

c. I understand that I must have at least a successfully completed investigation (NAC, NACI, ENTAC, NACLAC) for authorization to receive an account to connect to the Network.

d. Magnetic disks or diskettes will not be removed from the computer area without the approval of the IASO/IMO or supervisor.

6. I will not move hardware or alter communication connections without first getting approval from the SA or IASO/IMO.

7. I will scan all magnetic media for malicious software (viruses) with an Antivirus software before loading it onto a FORT KNOX system or network.

8. I will not forward chain-mail or virus warnings. The Army Computer Emergency Response Team issues virus alerts and threat advisories to the DOIM and the DOIM will issue to the Fort Knox Community. I will report chain-mail or virus warnings to my IASO/IMO and delete the message with their direction. I will not attempt to run "sniffer," "password cracker" or other hacker-related software on the network.

9. I know I am subject to disciplinary action per punitive regulations for any abuse of access privileges.

10. If I observe anything on the system I am using that indicates inadequate security, I will notify the IASO/IMO. I know what constitutes a security incident and know that I must immediately report such incidents to the IASO/IMO.

11. I will comply with security guidance issued by my system administrator and IASO.

I understand this agreement and will keep the system secure. If I am the IASO/IMO, I will ensure that all users in my area of responsibility sign this agreement.

USER'S FULL NAME (TYPED OR PRINTED):

USER'S SIGNATURE/DATE SIGNED:

ORGANIZATION:

IASO'S FULL NAME (TYPED OR PRINTED):

IASO'S SIGNATURE/DATE SIGNED: