# FORT KNOX INSTALLATION CAMPUS AREA NETWORK
# SECRET INTERNET PROTOCOL ROUTER NETWORK ACCEPTABLE USE POLICY

For use of this form, see AR 25-2; ALARACT 158/2008; and IA Controls ECIM-1, PRAS-2, PRTN-1, and VIIR-2

1. SCOPE. This policy applies to all Soldiers, civilians, and contractors who use a U.S. Government (USG) information system (IS) that is supported and serviced by the Fort Knox Network Enterprise Center (NEC). The scope of this document includes the Fort Knox Installation Campus Area Network (FKICAN) Secret Internet Protocol Router Network (SIPRNET), computers, Portable Electronic Devices (PEDs), and services.

2. CONSENT PROVISION: By signing this document, I acknowledge and consent that when I access Department of Defense (DOD) information systems:

a. I am accessing a USG IS (which includes any device attached to this IS) that is provided for USG authorized use only.

b. I consent to the following conditions:

(1) The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

(2) At any time, the USG may inspect and seize data stored on this IS.

(3) Communications using, or data stored on this IS are not private; are subject to routine monitoring, interception, and search; and may be disclosed or used for any USG-authorized purpose.

(4) This IS includes security measures (e.g., authentication and access controls) to protect USG interests -- not for personal benefit or privacy.

(5) Notwithstanding the above, using an IS does not constitute consent to PM, LE, or CI investigative searching for monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergies and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, USG actions for purposes of network administration, operation, protection, or defense or for COMSEC. This includes all communications and data on an IS, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including PM, LE, or CI investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for PM, LE, or CI investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with (IAW) established legal standards and DOD policy. Users are strongly encouraged to see personal legal counsel on such matters prior to using an IS if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data they assert are protected by any such privilege or confidentiality. However, users' identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DOD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DOD policy. However, in such cases, the USG is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data and legal protections regarding the use and disclosure of privileged information; such communication and data are private and confidential. Further, the USG shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(6) In cases when the user has consented to content searching or monitoring of communications or data for PM, LE, or CI investigative searching (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the USG may, solely at its discretion and IAW DOD policy, elect to apply a privilege or other restriction on the USG's otherwise authorized use or disclosure of such information.

(7) All of the above conditions apply, regardless of whether the access or use of an IS includes the display of a Notice and Consent Banner ("banner"). When a banner is used, it functions to remind the user of conditions that are set forth in this User Agreement, regardless of whether it expressly references this User Agreement.

3. ACCESS. Access to the USG IS and/or FKICAN SIPRNET is for official, authorized use as set forth in DOD 5500.7-R; Joint Ethics Regulation; AR 25-2; and any further limitations this policy may establish.

4. REVOCABILITY. Access to the USG IS and/or FKICAN SIPRNET resources is subject to monitoring and security scans for Information Assurance Vulnerability Alert compliance and is a revocable privilege.

5. MINIMUM SECURITY RULES AND REQUIREMENTS. As a user of a USG IS and/or the FKICAN SIPRNET, I will adhere to the following minimum security rules:

a. I will not be permitted access to any network unless I am in complete compliance with personnel security standards outlined in AR 25-2 and local policies.

b. I will participate in all training programs, as required (inclusive of threat identification, physical security, acceptable use policies, security awareness, malicious content and logic identification, and non-standard threats such as social engineering). A copy of my completion certificates will be provided to my Information Management Officer (IMO).

c. I am responsible for all activities that occur under my individual account once my password has been issued to me. I will generate, store, and protect my password IAW AR 25-2. I understand that my password is classified SECRET.

d. I will only use authorized hardware and software. I will not install, connect, or use any personally-owned hardware, software, shareware, or public domain software. I will not connect any personal IT equipment (i.e., PEDs, PDAs, personal computers, USB devices, and digitally-enabled devices) to my USG IS or to any USG network.

e. I will use virus-checking procedures before uploading or accessing information from any USG IS, diskette, attachment, compact disk, USB, or external drive.

f. I will use operating systems and programs only as specifically authorized, ensuring they are not altered, changed, or re-configured.

g. Computer equipment maintenance will only be performed by a NEC-recognized/approved source.

h. While powered on, I will not leave my computer unattended. If the area is approved for open storage, I will log off the computer when leaving the work area. For areas not approved for open storage and in all cases at the end of each work day, I will power down the system and secure the appropriate devices.

i. I will immediately report any suspicious output, files, shortcuts, or system problems to the FKICAN SIPRNET System Administrator and/or Information Assurance Security Officer (IASO). If I observe anything on the IS I am using that indicates inadequate security, I will immediately notify the FKICAN SIPRNET IASO. I have read the Fort Knox Information Assurance (IA) Incident Response Policy, so I know what constitutes a security incident and that I must immediately report such incidents to the FKICAN SIPRNET IASO.

j. I will ensure that only one connection to the FKICAN SIPRNET on a USG IS is enabled at any given time-any combination of two or more simultaneous connections (i.e., direct connect, modem, or wireless) is strictly prohibited.

k. I will not connect wireless or Bluetooth devices to USG equipment.

l. I will not use my USG e-mail address on any private or public web site except when necessary to conduct business in an official Government capacity.

m. I will ensure any quotes that are part of my e-mail signature block are professional in nature.

n. I will not utilize any media to transfer data from a classified IS to an unclassified IS.

o. I will ensure data does not exceed the security classification level for which the IS has been approved.

p. The IS classification level for the FKICAN SIPRNET is SECRET. I will not attempt to access or process data exceeding this authorized level.

q. I will power down the system when there are non-cleared personnel in the area.

r. I will mark all media introduced into the FKICAN SIPRNET as SECRET, regardless of the implied classification of the data. This media will be maintained and destroyed IAW AR 380-5.

s. I understand the following activities define UNACCEPTABLE uses of a USG IS:

- Accessing pornography, obscene material, or any other inappropriate content.
- Gambling.
- Transmitting chain letters. This includes warnings about the "latest virus" with instructions to forward to everyone you know.
- Advertising, soliciting, or selling for commercial or private gain.
- Using unauthorized peer-to-peer software (i.e., Gnutella, Napster, iTunes, Kazaa, Limeware) to download MP3 music, video files, games, etc.
- Copyright infringement (i.e., unauthorized copying/distribution of software, music, books, photographs, etc.)

- Any unlawful conduct.
- Web blogs.
- Personal use other than as authorized by both the designated approving authority and my supervisor.
- Streaming data or tickers from the internet (automatic download programs that keep abreast of stock prices, sports scores, and news) (i.e., e-trade, ESPN, CNN, Weatherbug, live audio/video, etc.)
- Internet game play (i.e., Fantasy Football, Scrabble, Quake, etc.)
- Forwarding official e-mail to non-official accounts or devices.
- Internet Chat or instant messenger services (i.e., AOL, MSN, Yahoo, etc.) except for AKO-S chat, which is an Army-authorized chat forum.
- Introduction of executable (i.e., .exe, .vbs, or .bat files, etc.) or malicious code.
- Using USG systems to bid on online auctions or receive personal payments, prizes, and giveaways.

t. I understand that all PEDs, i.e., cell phones, pagers, etc., are prohibited in areas where classified information is processed.

u. Writing to removable media such as USB and DVD/CD drives is prohibited on SIPRNET without express authorization from the DAA. Read only privileges are not impacted and are allowed for DoD personnel based on existing procedures, need-to-know and mission need.

v. I understand that I will not write to removable media on SIPRNET, such as USB or DVD/CD drives unless specifically authorized, in writing to do so by my Command.

6. ENFORCEMENT. Any personnel found violating this policy may be subject to disciplinary actions as outlined in the Uniform Code of Military Justice (UCMJ) or under other disciplinary administrative or contractual actions, as applicable. Personnel who fail to comply with these requirements and are not subject to UCMJ will be subject to disciplinary, administrative, or prosecutorial actions as authorized from criminal or civil sanctions under sections including, but not limited to, the United States Code, contractual support obligations, or Federal or state regulations.

7. ACKNOWLEDGEMENT. I have read the FKICAN SIPRNET SOP, FKICAN Computer User Guide, and FKICAN Incident Response Policy, and above requirements regarding use/access to the FKICAN SIPRNET. I understand my responsibilities regarding the protection and use of these systems and the information contained in them. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

I understand that I have the following responsibilities:

a. If authorized and approved to utilize "write" capabilities on SIPRNET, I understand that I must utilize the two person integrity (TPI) rule.

b. I must keep a log of each and every data transfer and ensure all required log items are completed, and that the second person under the TPI rule will witness each and every data transfer and complete log as a witness.

c. I understand that AR 25-2 is the implementation of Federal Law and is punitive in nature. Violations of paragraphs 3-3, 4-5, 4-6, 4-12, 4-13, 4-16, 4-20 and 6-5 of this regulation may be punishable as violations of a lawful general order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative or contractual actions as applicable. Personnel who are not subject to UCMJ who fail to comply with these requirements may be subject to disciplinary, administrative or prosecutorial actions.

8. POINT OF CONTACT. The POC for this policy is the Installation Information Assurance Manager, NEC.

**NOTICE: Expires 1 year from date of signature. Annual authentication is required.**

LAST NAME, FIRST NAME, MI:

RANK/GRADE:

PHONE NUMBER:

UNIT/DIRECTORATE/ACTIVITY:

AKO E-MAIL ADDRESS:

SIGNATURE:

DATE:

IASO'S SIGNATURE:

DATE: