Acceptable Use Policy (AUP)
for
Presidio of Monterey
Installation Campus Area Network (ICAN) and Classified Campus Area Network (CCAN)
Version 2.0

Reference: AR 25-2 (Information Assurance). A well-protected DoD/Army network enables organizations to easily handle the increasing dependence on the Internet. For a DoD/Army organization to be successful, it needs to integrate information that is secure from all aspects of the organization. The purpose of this policy is to outline the acceptable use of computer equipment within the Presidio of Monterey ICAN and the DoD/Army network. These rules are in place to protect the employee and the organization. Inappropriate use exposes DoD/Army units to risks including attacks, compromise of network systems, and legal issues. This policy applies to all employees, contractors, consultants, temporary employees, and other workers assigned to the Presidio of Monterey.

---

1. Understanding. By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

a. You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

b. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system 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 U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

(5) Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(a) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all

Initials

communications and data on an information system, regardless of any applicable privilege or confidentiality.

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

(c) 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 established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(d) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's 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.

(e) 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 U.S. Government 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.

(f) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government 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 personnel misconduct, law enforcement, or counterintelligence 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 U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government'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 information system includes the display of a Notice and Consent Banner ("banner"). When a banner

Initials

is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

c. I understand that I may only use Government resources, to include Government communications systems and equipment, such as Government-owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems paid for by the Government, for official use and authorized purposes. I further understand that I am responsible for safeguarding the information contained in the Presidio of Monterey Campus Area Network (ICAN), the Defense Information Systems Agency (DISA) Unclassified but Sensitive Internet Protocol Routing Network (NIPRNET), and the Secret Internet Protocol Routing Network (SIPRNET) from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

2. Access. Access to these networks is for official use and authorized purposes as set forth in DoD 5500.7-R, Joint Ethics Regulation (JER); AR 25-1, Army Knowledge Management and Information Technology; AR 25-2, Information Assurance; AR 380-5, Department of the Army Information Security Program and this policy.

3. Revocability. Access to Army resources is a revocable privilege. Access may be revoked for any violation of the Acceptable Use Policy or any action that puts the POM ICAN and/or the DoD Network at risk. Network access will be re-instated only after the following conditions have been met:

a. The user involved has re-taken and completed the DoD Cyber Awareness Challenge Training.

b. The user involved has re-signed the POM ICAN AUP.

c. The user's Commander has requested re-instatement of the user's network access.

4. Classified information processing. The SIPRNET is the primary classified Information System (IS) for the POM. The SIPRNET is a US-only system approved to process secret or lower level information. The SIPRNET is not authorized to process TOP SECRET information.

a. The SIPRNET provides communication to external Department of Defense (DoD) organizations. Primarily this is done via electronic mail (email) and internet networking protocols.

b. The classification boundary between the SIPRNET and the NIPRNET requires vigilance and attention by all users. The SIPRNET is a US-only system and is not accredited for transmission of NATO material.

Initials

c. The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the SIPRNET is a security violation and will be investigated and handled as a security violation or as a criminal offense.

d. Personnel are not permitted access to the CCAN unless in complete compliance with POM personnel security requirements and have been approved for access.

---

5. Unclassified information processing. The NIPRNET is the primary unclassified information system for the organizations and personnel assigned to POM.

a. The NIPRNET provides unclassified communication to external DoD and other United States Government organizations. This is done via email and Internet networking protocols.

b. The NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information. The NIPRNET is NOT approved to process classified information.

c. The NIPRNET and the Internet, as viewed by Designated Approving Authority (DAA), are synonymous. Email and attachments to email are vulnerable to interception as they traverse the NIPRNET and the Internet.

---

6. Minimum-security rules and requirements. Personnel are not permitted access to the NIPRNET unless they comply with the requirements of AR 25-2, Information Assurance; AR 25-1, Army Knowledge Management and Information Technology Management; AR 380-5, Department of the Army Information Security Program.

---

7. Personnel responsibility statement. I agree to the following security rules and requirements:

a. I will complete initial and annual Information Assurance (IA) Awareness training, aka DoD Cyber Awareness Challenge Training, and participate in all training programs as required (including Personal Identifiable Information (PII); Data-At-Rest (DAR), Phishing, encryption, road warrior, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before and after receiving system access.

b. I understand that I am responsible for any and all activity that occurs under my assigned ICAN account. I am the only authorized user of this account. I will not share my Common Access Card (CAC) or reveal my Personal Identification Number (PIN) to anyone. I will notify the POM Information Assurance Manager (IAM) immediately of any breaches of access.

c. I understand that if my user account is not used to log into the POM network for a period of **30 days or more**, the account will be disabled. At the 45-day period of inactivity, the account will be deleted. I am responsible for coordinating with my Supervisor to ensure the POM NEC gets notified if I will be on extended TDY, sick leave etc. to avoid network/email account deletion.

Initials

d. As a general user I will logon to the ICAN using a Common Access Card (CAC) unless a waiver is granted for me to logon with a username and password. If I am granted access to logon with a username and password I will follow password guidance as specified below.

e. I will create passwords in accordance with the following guidance: My password will consist of at least 15 characters with a minimum of 2 each of uppercase and lowercase letters, numbers, and special characters. I will not use a word found in the dictionary, thesaurus or list (English or foreign); my name; names of family, pets, friends, co-workers, or fantasy characters; computer terms and names, commands, sites, companies, hardware or software; common words such as "sanjose", "sanfran" or other derivative; birthdays, addresses, phone numbers or other personal information; word or number patterns like "aaabbb", "qwerty", "mypassword", or "abcde12345"; or spell any words backwards or precede or follow a word with a digit (e.g., secret 1, 1 secret); military slang, acronyms, descriptors, call signs or system identification. I understand that I must change my password every 60 days.

f. I will adhere to all Information Assurance Vulnerability Alert (IAVA) requirements and directions that may be given by the Network Enterprise Center (NEC), such as directions to logoff and leave my computer powered on at the end of the duty day. Information Assurance Vulnerability Management (IAVM) is the Army's proactive approach to maintaining, patching, and updating systems before exploitation. This proactive approach allows the availability of secure and accurate information to reach all service members and DoD employees. IAVA is the method used to alert all installations of possible exploitation to DoD Information Systems and corrective action needed.

g. I understand that if my government issued PC is not connected to the POM network and powered on for a period of **30 days or more**, that my system will be disabled from the network. If this happens, I will have to coordinate with the POM NEC to request that my system be re-imaged and re-added to the POM ICAN. The system will be deleted after 45 days of inactivity.

h. I will ensure that any and all sensitive and Personally Identifiable Information (PII) stored on my system is stored in the EFS encrypted folder created inside my "Documents" folder called "EFS". Individuals who do not take proper steps to protect sensitive data are subject to administrative, disciplinary, and or criminal penalties. I will contact my organization's IT representative if I do not understand the use of the EFS encrypted folder.

i. I will use only authorized hardware and software.

(1) I will not download, install, or use any unauthorized software, including unauthorized peer-to-peer software, such as Kazaa, Limeware, eDonkey, Napster, Skype, and Bittorent.

(2) I will not connect or install personal, non-government owned, or unauthorized government owned computing systems or devices including but not limited to USB devices, external media, personal laptop, contractor-owned laptop, stand alone systems and mobile communication devices to the POM ICAN without prior written approval from the Designated Approving Authority (DAA).

Initials

(3) I will not install any personally owned software on my government computer.

j. I will use virus-checking procedures before uploading or accessing information from any system, removal media, attachment, or web site. Every system will run NEC approved virus protection software with the latest virus definition file.

k. I will not attempt to access or process data exceeding my authorized Information Security classification level. I will not process or transmit classified information on the NIPRNET.

l. I will safeguard and mark with the appropriate classification level/handling markings all information created, copied, stored, or disseminated from the Information System (IS) and will not disseminate it to anyone without a specific need to know.

m. I will secure my government-owned issued laptop, blackberry and other portable electronic devices when not in use and not in my possession.

n. I will not alter, change, configure, or use any hardware, operating systems or programs without prior written approval from the NEC.

o. I will not disable or remove security or protective software and other mechanisms and their associated logs from any information system.

p. I will not introduce executable code (i.e. .exe, .com, .vbs, or .bat files) without prior written approval from the NEC, nor will I write malicious code.

q. I will not utilize Army or DoD provided ISs for commercial/financial gain or illegal activities.

r. I understand that only a System Administrator or an authorized technician may perform hardware and software installations and maintenance.

s. I understand my workstation will lock automatically after ten minutes of inactivity. If departing the area, I will log off or lock the workstation and remove my CAC.

t. I will immediately report any suspicious output, files, shortcuts, links, or system activities to the NEC Help Desk at 242-5028 and the Installation Information Assurance Manager (IIAM) at 242-7181 and cease all activities on the system.

u. I will address any questions regarding acceptable use or information assurance to the IIAM at 242-7181.

v. In addition to the specific prohibitions outlined in AR 25-1, I understand that the following activities are **not** acceptable uses of an Army IS and are prohibited:

(1) The use of hacker or hacker-related software on any system.

(2) The intentional introduction of a virus, worm, or a Trojan horse on any computer or network.

Initials

(3) The intentional breaking into, damaging, defacing, or destroying any hardware or software system belonging to another person, activity, agency, or entity.

(4) Accessing, downloading or storing pornography or obscene material (adult or child) without an official purpose.

(5) Accessing gambling related sites without an official purpose.

(6) Downloading, or copying copyright-protected software, literature, music or video, except as authorized under the Fair Use Doctrine.

(7) Accessing, downloading, or copying hate speech or materials that ridicule or discriminate against others on the basis of race, creed, religion, color, gender, disability, national origin, or sexual orientation without an official purpose.

(8) Any use that could cause congestion, delay, or degradation of service to any Government IS, to include:

(a) Unofficial Streaming Video or Audio

(b) Unofficial Internet radio

(c) Unofficial Chat Rooms

(d) Unofficial Instant Messaging (IM) Software (AKO and DCO chat are the only authorized IM methods)

(e) Information that is continually updated from the internet, such as stock quotes, weather, time, etc.

(f) Internet Interactive Games

(9) Political transmissions, including, but not limited to, transmissions that advocate the election of particular candidates for public office.

x. I understand that the following activities are considered acceptable uses of an Army IS and are generally authorized at POM, provided the use is of reasonable duration and frequency and does not adversely affect the performance of official duties; involve commercial gain or the operation of a personal business enterprise; reflect adversely on POM, DA, or DoD; overburden the ICAN or the NIPRNET; create any significant additional cost to POM:

(1) During duty hours:

(a) Checking in with your spouse or minor children.

(b) Scheduling medical/dental appointments.

(c) Sending E-mails to build office morale by keeping employees informed of office activities.

(d) Browsing for professional information having relevance to your official duties.

Initials

(2) During lunch/non-duty hours:

(a) Arranging for home/auto repairs.

(b) Brief visits/searches to acceptable Internet sites for personal use.

y. I will not store or transmit personnel medical data or privacy act material without proper encryption or other safeguards.

z. I will not use e-mail to:

(1) Create, download, store, copy, transmit, or broadcast chain letters.

(2) "Spam" to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.

(3) Broadcast unsubstantiated virus warnings or messages from sources other than approved NEC, DA, or DoD sources.

(4) Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting smaller specifically interested populations unless specifically approved and configured by the POM NEC.

aa. I will not use my personal/commercial e-mail to conduct official government business.

bb. I will not forward official mail to non-official accounts or devices.

Initials

NOTE: Items 8, 9, 10, 11, and 12 require acknowledgement as well. ALL users are required to initial below each item regardless of whether they are currently assigned or using such services/devices/access. This will acknowledge having read the policy requirements should the user be issued or use such services/devices/access in the future.

8. Laptop Users. Mobile Computing Devices (MCD) such as laptops pose unique security challenges. Users of these information systems (IS) are tasked with the physical security of these devices and must protect the IS from compromise when used as a standalone system, when traveling or remotely connected.

a. I understand that if my Government issued laptop is NOT connected and logged into the POM network for a period of **30 days or more**, my system account will be disabled from the network. If this occurs, I will be required to contact my organization's IT representative to submit a request to the POM NEC to have the system re-imaged and re-added to the POM Network. The system will be deleted from the network after 45 days of inactivity.

b. I understand I must coordinate with the POM NEC in advance to notify them if my system will be disconnected from the network for a **period exceeding 30 days** due to travel, TDY, etc. If I fail to provide this information, my system may be deleted from the network and my network access denied.

c. I understand that I must coordinate with my supervisor to notify the POM NEC if my user network account will not be used for any reason for a period of **30 days or more** such as leave, TDY, etc.

d. I understand that if my user account is not used to log into the POM network for a period of **30 days of more**, the account will be disabled. At the 45-day period of inactivity, the account will be deleted.

e. **If my laptop PC is configured for use as a "Road Warrior" travel system, I will refer to the section below titled "Road Warrior" Laptop Security and acknowledge agreement by signing below.

f. I understand that I shall secure the Government issued laptop at all times when not in use or in my possession. I will report the loss of my laptop immediately to the IIAM at 242-6847, and/or the POM Information Assurance Officer (IAO) at 242-6847, who in turn will report this information to the appropriate Commander(s), intelligence, and law enforcement representatives immediately.

g. I will ensure that any and all sensitive and Personally Identifiable Information (PII) stored on my system is stored in the EFS encrypted folder created inside my "Documents" folder called "EFS". Individuals who do not take the proper steps to protect sensitive data are subject to administrative, disciplinary, and or criminal penalties. I will contact my organization's IT representative if I do not understand the use of the EFS encrypted folder.

Initials

9. "Road Warrior" Laptop Security. Laptops configured as "Road Warrior" devices pose unique challenges. Users are tasked with ensuring their security by following the requirement outlined below per the "Road Warrior "Laptop Security Version 1.3 Best Business Practice (BBP) Update 18 Mar 09.

a. I will secure the laptop/tablet at all times when not in use or in my possession and will never leave it unattended in public, meetings, conventions, or conferences.

b. I will use non-descript carrying cases that do not display my organization, military affiliation or company's logo.

c. I will never place my laptop/tablet in checked or unattended baggage.

d. I will never leave my laptop/tablet unattended in a vehicle where it can be seen.

e. I will anchor my laptop/tablet to a fixed object during hotel stays using a cable lock provided by my organization.

f. I will include a business card or similar identifier affixed to the laptop/tablet or in the carrying bag to help identify the device in case of loss.

g. I will remove and secure removable PC cards and peripheral devices when not in use.

h. I am responsible for ensuring my CAC login credentials are valid for the length of time the laptop/tablet is disconnected from the POM network or while traveling.

i. I will coordinate with the POM NEC to update my laptop/tablet anti-virus, patching, upgrades, etc. if I will be disconnected from the POM network for more than 14 days.

Initials

10. Remote Access. Remote access to the POM ICAN will be via Virtual Private Network (VPN. Government owned hardware and software will be used. The employee is the only individual authorized to use this equipment. VPN access accounts will be as authorized by the supervisor and approved by the POM NEC. Requirements as indicated throughout this AUP are applicable for access to USG resources.

Initials

11. Blackberry devices.

a. I will be held responsible for damage caused to a Government system or data through negligence or a willful act.

b. I am not authorized and will not use Bluetooth technology with Blackberry devices except for the authorized CAC sled found on the Army approved two way wireless email device listing.

c. I will not operate a wireless device within 100 feet of any areas where Classified information is electronically stored or processed.

d. I understand that all charges incurred in excess of the normal monthly service charge will be the responsibility of the Blackberry user. Charges will be incurred for the following misuses of the device: exceeding allocated minutes per month, use of text messaging; neglect or abusive damage to the device or accessory.

e. I understand that the use of the Government issued Blackberry device is **for official use only**. I will not modify the settings of the device or software in any manner to facilitate the use of commercial e-mail systems.

Initials

12. SMS (Short Messaging Service) on Blackberry\Wireless devices "Text Messaging"

I am aware of the following risks when utilizing the SMS (Text Messaging) service:

a. Messages are not encrypted and copies are stored in memory on the phone and in the wireless carrier database. Sensitive information should not be sent via SMS/Text/Messages/Multimedia Messaging Service (MMS).

b. Links to hacker web sites can be sent to a SMS/Text Message/MMS. If a user connects to the site address, malware could be downloaded on the phone.

c. Executable files (including malware) can be embedded in SMS/Text Message/MMS.

d. Photos sent via SMS/Text Messages/MMS can have links to hacker web sites embedded in the photo. When the photo is viewed, the phone will connect to the embedded website.

e. Photos sent via SMS/Text Messages/MMS can have executable files (including malware) embedded in the photo. When the photo is viewed the phone will execute the file.

f. I will utilize/send SMS (text) messaging for official use only.

Initials

13. Privacy Act Notice. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose the information could result in denial of access to POM Information Systems.

Initials

14. Acknowledgement. I have read and will comply with the above requirements regarding use of the POM Information Systems. I understand my responsibilities regarding these systems and the information contained in them.

Directorate, Office, Branch, School

Office Symbol, Building #, Room #

Phone Number

Last Name, First Name, MI

Rank/Grade

Signature

Date