DEPARTMENT OF THE ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, US ARMY GARRISON, PRESIDIO OF MONTEREY
1759 LEWIS ROAD, SUITE 210
MONTEREY, CA 93944-3223

REPLY TO
ATTENTION OF

IMPM-ZA

JUL 26 2016

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum #25-1, Wireless Device Policy

1. References:

a. AR 25-2, Information Assurance (RAR), 23 March 2009.

b. DoD 5500.7-R, Joint Ethics Regulation, 17 November 2011.

c. AR 25-1, Army Knowledge Management and Information Technology, 25 June 2013.

d. AR 735-5, Policies and Procedures for Property Accountability, Rapid Action Review (RAR) 22 August 2013.

e. HQDA Memo, Subject: US Army Guidance on the Use of Commercial Mobile Devices (CMD), 11 September 2013.

f. DA PAM 25-1-1, Army Information Technology Implementation Instructions, 26 September 2014.

2. Purpose: This memorandum establishes command policy for the acquisition and use of wireless devices including cellular telephones, pagers and personal data assistants (PDA) like the Blackberry e-mail device for United States Army Garrison (USAG), Presidio of Monterey (POM).

3. Applicability: This policy applies to all USAG personnel. This policy supersedes previous versions.

4. Proponent: The Deputy to the Garrison Commander (DGC) will designate and supervise the Garrison Information Management Officer (IMO) who will manage and administer the wireless device authorizations, monitor and validate authorized usage, and authorize bills for payment. Until a full time IMO is hired, the Garrison Resource Management Office will carry out the IMO duties. The point of contact is Mr. Dan Dieli, (831) 242-5984/DSN 768-5984.

5. Policy: Wireless devices will be provided only as required to meet the Garrison mission and duties assigned. These devices enhance the efficiency and effectiveness

of Garrison mission operations and provide rapid communications where needed. Because of its high cost, close management and control over their use is required. Garrison Directors, Management and Support Office Chiefs, or Division Chiefs must validate, approve and monitor wireless device requirements for their subordinates.

6. Action:

a. Directors, Management and Support Office Chiefs and Division Chiefs will:

(1) Approve wireless devices and service plans for their employees to accomplish their official duties and submit a signed Authorization Request for Wireless Device (Appendix A), available online at www.monterey.army.mil/RMO/resource_mgmt.html, to the IMO for action.

(2) Disapprove requests for wireless devices if the requested instrument is to be used for any of the following purposes:

(a) Used solely for the user's convenience or personal use without operational necessity or used to replace their personally owned wireless device.

(b) Used in lieu of official available fixed telecommunications systems (e.g. DSN, LAN lines, etc.).

(3) Oversee the use of wireless devices within their organizations and ensure appropriate action is taken when cases of unauthorized use are suspected or identified.

b. The Garrison IMO will:

(1) Procure and issue wireless devices and maintain a database including:

(a) Name, organization and duty position of person assigned a wireless device.

(b) Type of wireless device issued and the assigned phone number.

(c) Date of issuance and whether it is permanent or temporary.

(d) Wireless service plan provided and the plan cost.

(e) Date wireless device was returned, disconnected, suspended, reassigned or upgraded.

(2) Require users to read the Acceptable Use Policy (AUP-Appendix B) acknowledging that they have read and understand proper use of wireless devices and their responsibility to reimburse the Government for unauthorized use

(3) Require users to sign an AUP for the wireless device.

(4) Review itemized wireless device bills for unofficial or improper use. When necessary, require organizations/directorates to justify or reimburse expenses for unofficial calls. The IMO will coordinate any required collections through Garrison Resource Management.

(5) Compile statistics on wireless device use and prepare a monthly report to the DGC. These statistics will be used to revalidate wireless devices and determine service plans changes.

(6) Perform an annual audit of wireless devices to ensure they are:

(a) Accounted for and in the possession of the individual to whom it is assigned.

(b) In good working order.

(c) Returned when no longer needed and the service plans discontinued. The user will be required to re-sign the AUP when turning in wireless devices as they are considered durable property.

(d) Provide life cycle management and replace devices with an upgraded model provided at no cost in accordance with (IAW) the applicable service plan.

(7) Serve as the subject matter expert (SME) and primary command point of contact for all issues concerning wireless device use within POM.

c. Authorized Wireless Device Users will:

(1) General. Use the government wireless device IAW the principles of acceptable use for wired devices such as desktop, laptop or other computers, telephones, facsimile machines or other common office devices.

(2) Equipment and Service Plans. Be provided the minimum equipment and service plan required to perform official duties. This includes use while traveling on Government business for the purpose of notifying family members of any schedule or transportation changes and of safe arrivals and departures, use while TDY or working

off-site for extended periods when use of LAN lines is not possible; use to enhance the professional skills and knowledge of Garrison employees or to aid in the performance of duties.

7. Personal Use: It is unwarranted to require individuals authorized and required to carry a wireless device to also carry a personal device for routine communications. IAW references (a) and (f), wireless device use is permitted for brief communications of a personal nature for the purpose of checking on family, scheduling appointments (e.g. doctor, auto, home repair, etc.), brief Internet searches, e-mailing directions or sharing non-work related information, etc. Such personal communications are permitted as long as they:

a. Do not adversely affect the performance of official duties.

b. Are of reasonable duration (normally five minutes or less) and frequency (normally a few times a day), and are made during breaks, lunch periods or other off-duty periods.

c. Do not result in the user exceeding their authorized service plan. Users should consult the IMO to find out the details of the specific service plans for their wireless device.

8. Prohibited uses include:

a. Calls, e-mail or web searches that would reflect negatively on the Garrison and U.S. Army, such as sexually explicit and/or pornographic communications, images, or audio files; expressions of sexual or other forms of harassment; unofficial advertising, soliciting or selling intended for personal financial gain; or any form of gambling.

b. Activities inconsistent with DoD/Garrison policy or that violates other Army policies or laws such as: violating intellectual property and copyright law; supporting or promoting political agendas and/or candidates; or expressing subversive content incompatible with public service or in support of terrorist or subversive activities.

c. Actions that result in the theft of or abuse of wireless devices and/or services which cause unauthorized access, use, transfer or tampering with electronic accounts and files of others which result in the disruption, interference or loss of the work of others including, but are not limited to:

(1) Creating, downloading, storing, copying, transmitting or broadcasting chain letters.

(2) Sending "spam" or "letter-bomb" emails/texts designed to transmit repeatedly or interfere with the recipients' use of e-mail or texting features; or transmitting e-mails/texts to large groups (entire organizations) instead of targeting the relevant audience, or disseminating large files over e-mail instead of using shared drives or AKO.

(3) Employing applications for personal use using: streaming data, audio, or video; malicious logic and virus development software, tools, and files; unlicensed software, games; Web altering tools/software; and other software that may cause harm to Government computers and telecommunications systems, or transmitting unsubstantiated virus warnings via e-mail/text from sources other than system administrators.

9. Cost Control: Users shall ensure costs are minimized and avoid additional usage charges.

a. Directory Assistance and transmission of pictures or images incur additional charges and should only be used when absolutely necessary to execute assigned duties and as authorized.

b. Users traveling outside of the United States on TDY, taking long personal vacations or any other circumstances in which they will not need or use their wireless plan for an extended period of time should contact the IMO to have their service plan temporarily suspended to avoid unnecessary charges.

c. Additional usage charges above the minimum service plan resulting from personal use are the responsibility of the user. Excessive or unauthorized personal use could result in the revocation of the wireless device authorization and/or disciplinary action.

2 Encls
Appendix A: Wireless Authorization
Appendix B: Acceptable Use Policy

LAWRENCE T. BROWN
COL, MI
Commanding

DISTRIBUTION: G

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
US ARMY GARRISON, PRESIDIO OF MONTEREY
1759 LEWIS ROAD, SUITE 210
MONTEREY, CA 93944-3223

REPLY TO
ATTENTION OF

IMPM-

MEMORANDUM FOR Information Management Officer/Wireless Device Control Officer (IMO/WDCO)

SUBJECT: Authorization Request for Wireless Device for *NAME*

1. _____(NAME) _____ is authorized the following wireless device and service plan required to perform official duties. Unless specified, the lowest cost equipment will be provided.

2. The following wireless device(s) and service plan(s) is authorized:

   a. **Smartphone** ☐ **Cellular Phone** ☐ **Pager** ☐ **Aircard** ☐ **Tablet PC**

      (1) **Specific device** ___ **(e.g. Blackberry Classic)** _____

   b. **Service Plan** ☐ Voice only ☐ Data Only ☐ Data & Voice

      (1) **Minutes per month** ☐ 450 ☐ 900 ☐ Other _____

3. International calling is ☐ / is not ☐ authorized.

4. After duty hours and temporary duty usage is ☐ / is not ☐ authorized.

Signature block

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, US ARMY GARRISON, PRESIDIO OF MONTEREY
1759 LEWIS ROAD, SUITE 210
MONTEREY, CA 93944-3223

REPLY TO
ATTENTION OF

Acceptable Use Policy (AUP) for Cellular and Satellite Telephone Devices

1. References:

a. AR 380-5, Department of the Army (DA) Information Security Program and this policy, 29 September 2000.

b. AR 25-2, Information Assurance (RAR), 23 March 2009.

c. DoD 5500.7-R, Joint Ethics Regulation, 17 November 2011.

d. AR 25-1, Army Knowledge Management and Information Technology, 25 June 2013.

e. AUP for Defense Language Institute Foreign Language Center and Presidio of Monterey Installation Campus Area Network (ICAN) and Classified Campus Area Network (CCAN) 7 Jun 2016.

2. Purpose. The purpose of this policy is to outline the acceptable use of wireless cellular devices and satellite phones for the U.S. Army Garrison, Presidio of Monterey (POM). This policy applies to all Garrison employees requiring issuance of wireless devices.

3. Policy. By signing this document, the user acknowledges and consents that when using Department of Defense (DoD) cellular and satellite telephone devices:

a. User is accessing cellular and satellite telephone device that is provided for U.S. Government authorized use only.

b. User consents to the following conditions:

(1) The provisions of reference (e) that apply to the ICAN or CCAN apply to all cellular and satellite telephone devices that interacts with the ICAN. A signed copy of reference (e) will be attached to this signed document for all users that connect to the ICAN or CCAN.

(2) User may only use Government resources, to include Government owned wireless devices for official use and authorized purposes.

Appendix B

4. Access. Access to cellular and satellite devices are for official use and authorized purposes as set forth in references (a) through (e).

5. Revocability. Access to Army resources is a revocable privilege. Access may be revoked for any violation of the AUP or any action that puts the ICAN at risk. Cellular and satellite telephone devices will be will be re-instated only after the following conditions have been met:

a. The user involved has re-taken and completed the Information Assurance (IA) Awareness training.

b. The user involved has re-signed the general and the cellular and satellite telephone devices AUP.

c. The user's supervisor has requested re-instatement of cellular and/or satellite telephone devices.

6. Personnel responsibility statement. User agrees to the following security rules and requirements:

a. User will complete initial and annual Information Assurance (IA) Awareness 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 cellular or satellite telephone devices.

b. User is responsible for any and all activity that occurs on the assigned wireless device. User is the only authorized user of this device. Users will not share Common Access Card (CAC) or reveal Personal Identification Number (PIN) with anyone. User will notify the POM Information Assurance Manager (IAM) immediately of any breaches of access.

c. Users will logon to the wireless device using a password and will follow password guidance as specified in the general AUP.

d. Users will ensure that any and all sensitive and PII is not emailed unless a digital signature and encryption is configured for that device.

_____
Initials

e. User will not attempt to access or process data exceeding authorized Information Security classification level. User will not process or transmit classified information on the wireless device.

f. User will secure government-owned wireless devices when not in use and not in their possession.

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

h. User will not utilize Army or DoD provided wireless device for commercial/financial gain or illegal activities.

i. User understands that only a System Administrator or an authorized technician may perform hardware and software installations and maintenance.

j. User understands the wireless device will lock automatically after inactivity and will not disable this feature.

k. User will address any questions regarding acceptable use to the Garrison Information Management Officer, Mr. Dan Dieli, Building 614, suite 142A, 831-242-5984, daniel.m.dieli.civ@mail.mil .

l. In addition to the specific prohibitions outlined in AR 25-2, User understands that the following activities are not acceptable uses of government equipment and are prohibited:

(1) The intentional introduction of a virus, worm or a Trojan horse on any wireless device.

(2) The intentional breaking into, damaging, defacing or destroying any wireless device belonging to another person, activity, agency or entity.

(3) Accessing pornography or obscene material without an official purpose.

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

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

(6) Accessing 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.

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

m. User understands that the following activities are considered acceptable uses of an Army Cellular device 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, DoD or 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.

(2) During lunch/non-duty hours:

(a) Arranging for appointments such as home/auto repairs.

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

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

o. User 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.

(a) User will not use personal/commercial e-mail to conduct official government business.

(b) User will not forward official mail to non-official accounts or devices.

(c) User will not configure or download their personal email account to the government issued Blackberry.

7. Blackberry Devices.

a. User will be held responsible for damage caused to a cellular device or data through negligence or a willful act.

b. User is 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. User will not operate a wireless device within 100 feet of any areas where classified information is electronically stored or processed.

d. User understands 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, neglect or abusive damage to the device or accessory, or loss of the device.

e. User understands that the use of the Government issued Blackberry device is **For Official Use Only**, and will not modify the settings of the device or software in any manner to facilitate the use of commercial e-mail systems.

8. SMS (Short Messaging Service) on Blackberry\Wireless devices "Text Messaging." User is 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 web site of 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.

9. 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 cellular and satellite telephone devices.

10. Acknowledgement. I have read and will comply with the above requirements regarding use of the Government issued cellular and satellite telephone devices. I understand my responsibilities regarding these devices and the information contained in them. I also understand and acknowledge what constitutes improper use and that I am subject to possible disciplinary action or financial obligation if I violate those guidelines and/or policies.

11. I was issued the following wireless device(s):

a. Device Type: _____
IMEI #: _____
Make/Model: _____
ICCID #: _____

b. Phone Number: _____

c. Service Plan Type: _____

 _____ Initials

Directorate, Office, Branch

Office Symbol, Building, Room

Phone Number

Last Name, First Name, MI

Rank/Grade

Signature

Date

Signature for Turn-In of Device

Date of Turn-In

Initials