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

APR 05 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum #20, Wireless Device Policy

1. References:

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

b. HQDA Memo, Subject: Updated Guidance on the Management of BlackBerry Devices with Internal Bluetooth Capability, 1 August 2006.

c. AR 735-5, Policies and Procedures for Property Accountability, 28 February 2005.

d. AER Supplement 1 to AR 25-1, Army Knowledge Management and Information Technology, 23 April 2006.

e. DoD 5500.7-R, Joint Ethics Regulation, 29 November 2007.

f. AR 25-1, Army Knowledge Management and Information Technology, 4 December 2008.

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

3. Applicability: This policy applies to all USAG personnel issued a wireless device.

4. Proponent: The Deputy 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 Resource Management Office (RMO) will carry out the IMO duties. The point of contact is Mr. Anthony Trujillo, (831) 242-7503/DSN 768-7503.

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 their high cost, close management and control over their use is required. USAG POM 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 Control Offices and Installation Support Offices will submit via email to the Wireless Device Control Officer (WDCO) the names of their staff requiring wireless device support and the point of contact from their organization to coordinate support.

(1) They will 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) The device should not be used solely for the user's convenience or personal use without operational necessity or used to replace their personally owned wireless device.

(b) The device should not be used in lieu of official available fixed telecommunications systems (e.g., DSN, landlines, etc.).

(3) They will oversee the use of wireless devices within their organization 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 to include the following.

(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 (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 a DA Form 3161, Request for Issue or Turn-In (Appendix C), for the wireless device.

(4) The device shall be returned when no longer needed and the service plan is discontinued. The user will be required to sign a DA Form 3161, Request for Issue or Turn-In, when turning in wireless devices as they are considered durable property.

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

(6) 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.

(7) Perform an annual audit of wireless devices.

(a) The audit will account for the device and insure it is in the possession of the recorded assignee.

(b) The audit will insure the device is in good working order.

(8) The IMO shall provide life cycle management and replace devices with an upgraded model provided at no cost in accordance with the applicable service plan.

(9) 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 in accordance with 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. The requestor shall 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 landlines 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. In accordance with references (a) and (b), 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 or Garrison policy or that violates other Army policies or laws such as: violating intellectual property and copyright law; supporting or promoting political agendas 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 or 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 or 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.

10. Retroactive Authorization: Within 180 days of the effective date of this policy, all current wireless device users will sign and submit an approved Wireless Device Authorization form (Appendix A) and Acceptable Use Policy (Appendix B) to the IMO and sign a DA Form 3161, Request for Issue or Turn-In.

Encls
as

JOEL J. CLARK
COL, SF
Commanding

DISTRIBUTION: G