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

AMIM-PMG-ZA (1oo) 2 July 2024

MEMORANDUM FOR USAG Presidio of Monterey

SUBJECT: United States Army Garrison (USAG) Presidio of Monterey (PoM), Command Policy #31 - Wireless Devices

1. References:

a. AR 25-1, Army Information Technology Management, 15 July 2019

b. AR 25-2, Army Information Assurance (RAR), 4 April 2019

c. AR 25-13, Army Telecommunications and Unified Capabilities, 11 May 2017

d. AR 735-5, Property Accountability Policies, 10 April 2024

e. DOD 5500.7-R, Joint Ethics Regulation, 17 November 2011

f. AD 2019-23 Memo, Subject: Allocation of Wireless Portable ElectronicDevices, 1 August 2019

g. DA PAM 25-1-1, Army Information Technology Implementation instructions, 15 July 2019

h. OPI 2023-017 Use of Text Messages on Mobile Devices

i. DoDI 8170.01 Online Information Management and Electronic Messaging, 24 August 2021

2. Purpose: This memorandum establishes Command Policy for the acquisition and use of wireless devices to include: cellular telephones, Wi-Fi Hotspots, personal data assistants (PDA's) and Smart Phones (Apple, Android, Blackberry) for the United Stares Army Garrison (USAG) Presidio of Monterey (PoM).

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

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

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

5. Action:

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

(1) Approve wireless devices and service plans for their employees and submita signed Authorization Request for Wireless Device to the Information Management Officer (IMO) for action.The form is available on the SharePoint Library under IMO Documents at: https://armyeitaas.sharepoint-mil.us/sites/IMCOM-ID-T-USAG-PoM/IMO%20Documents/Forms/AllItems.aspx

(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.

(2) Maintain a database, to include:

(a) Name, organization, and duty position of the employee issued a wireless device

(b) Assign phone number and type of wireless device issued

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

(d) Wireless service plan provided, along with the plan cost

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

(3) Require users to read and sign the PoM Acceptable Use Policy (AUP), which acknowledges the user's understanding of the policy, and that the user can be held accountable for reimbursement to the Government for any unauthorized use. The form is available on the SharePoint Library under IMO Documents at: https://armyeitaas.sharepoint-mil.us/sites/IMCOM-ID-T-USAG-PoM/IMO%20Documents/Forms/AllItems.aspx

(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 plan 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 the deviceis assigned.

(b) In good working order.

(c) Returned to the IMO when no longer needed. The user is required to e-sign their original AUP in the return device block on page 7, as wireless devices are considered to be durable property.

(d) Provide life cycle management and replace devices with an upgraded model (provided at no cost to the Government) in accordance with (IAW) and 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) Use the government wireless device IAW the principles of acceptable use forwired devices (ie: desktops, laptops, telephones, facsimile machines, or other

commonoffice electronic devices).

(2) 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 andknowledge of Garrison employees or to aid in the performance of duties.

6. 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.

7. Prohibited uses include:

a. When conducting government business DoD users of government-owned mobile devices and non-government-owned devices must use Microsoft Teams Chat for text messages as the designated fully managed DoD Mobile Enterprise System. For use on a non-government-owned mobile devices, Microsoft Teams Chat will be available as a managed application controlled by an enterprise management system.

b. When mission needs or the effective conduct of DoD business cannot be adequately supported by Microsoft Teams Chat, SMS texting may be used in accordance with DoDI 8170.01 (reference i). In such cases, a complete copy of the record must be forwarded to an official DoD electronic messaging account of the user within 20 days of the record’s original creation or transmission in accordance with Section 2911 of Title 44 U.S.C, and Component processes. The

complete copy of the record includes the content of the message and required metadata, and the record must be retrievable and usable in compliance with the applicable retention schedule approved by the Archivist of the United States.

c. 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.

d. 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.

e. 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/text to large groups (entire organizations) instead of targeting the relevant audience or disseminating large files over e-mail instead of using shared drives.

(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.

8. 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.

9. Proponent: The Information Management Officer is responsible for managingand administering wireless device authorizations, monitoring, and validating authorized usage, and authorizing wireless carrier invoice payments. POC: Information Management Officer, usarmy.pom.id-training.mbx.imo-office@army.mil


Digitally signed by ARTINO.DANIEL.S.
Date: 2024.07.02 08:00:54 -07'00'

DANIEL S. ARTINO
COL, AV
Commanding