



DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON
4551 LLEWELLYN AVENUE, SUITE 5000
FORT GEORGE G. MEADE, MARYLAND 20755-5000

IMME-AO

MAR 02 2018

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Fort George G. Meade Policy Memorandum #69, Commercial Mobile Wireless Devices

1. References:

- a. AR 25-13, Telecommunications and Unified Capabilities, 25 March 2013.
- b. Department of the Army Pamphlet 25-1-1, Army Information Technology Implementation Instructions, 26 September 2014.
- c. AR 25-1, Army Information Technology, 25 June 2013
- d. AR 735-5, Property Accountability Policies, 26 September 2016

2. Purpose: This memorandum establishes command policy for the acquisition and use of commercial mobile wireless devices within United States Army Garrison (USAG), Fort Meade.

3. Applicability: This policy applies to all USAG personnel.

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.

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 IAW 1c.

IMME-AO

SUBJECT: Fort George G. Meade Policy Memorandum #69, Commercial Mobile Wireless Devices

6. Scope: For the purpose of this memorandum, a wireless device is a commercial mobile wireless device operating on a service plan paid for with Army appropriated funds. Wireless devices include smartphones, cell phones, and electronic tablets with cell service capability, air cards, and MiFi hotspots enabled devices.

7. Guidance: All Directorates and supporting organizations will review and validate the need for wireless communications based on mission every two years. Minimally used wireless devices should be handled in accordance with reference 1c above.

8. Action:

a. Directors, Support Office Chiefs and supervisors 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 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.

(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 terminated, suspended, reassigned, or upgraded.

IMME-AO

SUBJECT: Fort George G. Meade Policy Memorandum #69, Commercial Mobile Wireless Devices

(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 Office.

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

(a) Record wireless data use of devices with zero data over the course of a quarter.

(b) Create a report for DGC and notify directors of non-data use.

(c) Use monthly report to track zero data use wireless devices.

(d) After 60 days of non-use, suspend wireless line until justification is given to maintain wireless device or to terminate wireless line.

(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 users are required to re-sign the AUP when turning in wireless devices.

(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 and include in annual Management Internal Control Program (MICP).

c. Authorized Wireless Device Users will:

IMME-AO

SUBJECT: Fort George G. Meade Policy Memorandum #69, Commercial Mobile Wireless Devices

(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) Will not send "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 instead of targeting the relevant audience, or disseminating large files over e-mail instead of using shared drives.

(3) Will not employ 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 or text from sources other than system administrators.

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

a. Users traveling outside of the United States on temporary duty, 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.

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

10. Point of contact: Michael E. Steele, (301) 677-5153, michael.e.steele3.civ@mail.mail.



THOMAS S. RICKARD
COL, IN
Commanding

DISTRIBUTION:

A