



DEPARTMENT OF THE ARMY  
HEADQUARTERS, JOINT READINESS TRAINING CENTER AND FORT POLK  
6661 WARRIOR TRAIL, BUILDING 350  
FORT POLK, LOUISIANA 71459-5339

AFZX-IM

MAY 04 2016

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum G6-03 – Command Policy on Use of Wireless Communication Devices.

1. References.

- a. Army Regulation (AR) 380-5, Department of the Army Information Security Program, 29 Sep 00 and FORSCOM supplement 1 to AR 380-5, 27 May 03.
- b. AR 25-2, Information Assurance, 24 Oct 07, Rapid Action Revision 23 Mar 09.
- c. United States Army Information Systems Engineering Command Secret Internet Protocol Router Network Technical Implementation Criteria (Version 6), Oct 10.
- d. AR 25-1, Army Information Technology, 25 Jun 13.
- e. Department of the Army Best Business Practice 09-EC-M-0010 (Version 4.0), Wireless Security Standards, 26 Jun 13.

2. Purpose. This policy defines guidance on the approved use of wireless communication devices, services, and technologies on the installation.

3. Applicability. All Fort Polk units assigned or attached and Installation activities.

4. Definition. Wireless technology permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use infrared (IR), acoustic, radio frequency (RF), and optical, but as technology evolves, wireless could include other methods of transmission.

- a. A wireless device includes, but is not limited to; government issued or privately owned cellular telephones, pager/messaging devices, computers, tablets, personal digital assistants (PDAs), portable electronic devices (PEDs), mobile computing devices (MCDs), keyboards, computer mice, or other devices containing wireless communications or connectivity.

AFZX-IM

SUBJECT: Command Policy Memorandum G6-03 – Command Policy on Use of Wireless Communication Devices.

b. A wireless personal area network (WPAN) is a system that provides electromagnetic communication connectivity over a few yards. Currently it uses RF (e.g., Bluetooth) or IR technology.

c. Although there are many benefits for allowing wireless technologies, wireless devices introduce an additional risk to the network that goes beyond that of traditional wired networks. Wireless data transmissions that are not encrypted or are inadequately encrypted could potentially be intercepted and read in a matter of seconds. The intercepted data can also be jammed or the signal can be redirected to rouge access points.

5. Policy. No wireless device may be taken into areas where classified information is discussed or electronically processed, unless specifically documented in the Certification and Accreditation Package and permitted as an exception by the Designated Approving Authority (DAA) and all classification, access, and encryption restrictions are enforced for the device as they would be for a classified device.

a. No wireless device may not be taken into the Installation Operations Center (IOC), the installation Sensitive Compartmented Information Facility (SCIF), or other designated SECRET or TOP SECRET work areas. Entrances to these areas are clearly marked "NO CELL PHONES ALLOWED BEYOND THIS POINT." The G2/S2, G3/S3, and assigned security managers will enforce this policy within their designated areas.

b. No wireless devices may be connected to any network or government computing system.

6. Responsibilities for acquiring government owned wireless devices.

a. All wireless device requirements are to be coordinated through the Fort Polk G6 and approved by the Chief of Staff.

b. The Fort Polk G6 is the authorized issuing authority for government owned wireless devices and maintains an inventory list.

c. Telephone Control Officer (TCO). Each mission staff section and MSC will designate a primary and alternate TCO by issuing orders that are updated annually. The TCO is accountable for all assigned government wireless devices within their section/unit.

AFZX-IM

SUBJECT: Command Policy Memorandum G6-03 – Command Policy on Use of Wireless Communication Devices.

7. Exceptions to policy. Requests for exceptions to this policy will be handled on a case-by-case basis by the Fort Polk G6.
8. Violations. Persons subject to the Uniform Code of Military Justice may be punishable under Article 92 or other applicable provisions for violations of this policy. Department of the Army Civilian employees may be subject to appropriate disciplinary actions initiated in accordance with AR 690-100, Chapter, 751, and the table of penalties. All other personnel who violate this policy may be denied access to Fort Polk facilities.
9. This policy supersedes and rescinds all previous policies and SOPs on this subject matter.
10. The point of contact for this policy is the ACofS G6 at commercial (337) 531-5995 or DSN 863-5995.



GARY M. BRITO  
Brigadier General, USA  
Commanding

DISTRIBUTION:

A+