



DEPARTMENT OF THE ARMY
UNITED STATES ARMY, EUROPE, AND SEVENTH ARMY
UNIT 29351
APO AE 09014-9351

AEAIM-A

11 August 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: BlackBerry Policy

This memorandum expires 11 August 2005.

1. This memorandum supersedes memorandum, HQ USAREUR/7A, AEAIM-A, 20 December 2003, subject: Army Europe BlackBerry Policy.

2. References:

a. Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules, 25 May 2001 (available at <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>).

b. Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems, 5 June 1999 (available at http://www.fas.org/irp/offdocs/DCID_6-3_20Policy.htm).

c. National Security Agency IDOC-002-03, Operational Systems Security Doctrine for the S/MIME Enhanced BlackBerry for Government, July 2003 (available at http://www.smimeblackberry.net/docs/SMIME_Blackberry_IDOC-002-03_July_signed.pdf).

d. DOD Directive 8100.2, Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004 (available at <http://www.dtic.mil/whs/directives/corres/html/81002.htm>).

e. AR 25-1, 30 June 2004, Army Knowledge Management and Information Technology Management (available at http://www.army.mil/usapa/epubs/pdf/r25_1.pdf).

f. AR 25-2, 14 November 2003, Information Assurance (available at http://www.army.mil/usapa/epubs/pdf/r25_2.pdf).

3. BlackBerry wireless handheld technology is being implemented throughout Army in Europe. These devices provide remote e-mail access to the LandWarNet (Unclass) in support of official business. Due to their ease of use and tight integration with existing infrastructure, BlackBerry devices are authorized for personnel to allow always-on access to e-mail. The infrastructure to support this technology will be implemented by the Army in Europe, but each using organization will pay for its own BlackBerry devices and services. Approval authorities for acquiring BlackBerry devices (listed in para 6) must consider the long-term cost to their organizations

This memorandum is available at <https://www.aeaim.hqusareur.army.mil/library/>.

AEAIM-A
SUBJECT: BlackBerry Policy

before approving the acquisition. BlackBerry devices should be acquired only for mobile personnel who depend on e-mail as a mission-critical tool in addition to their existing cell-phone capability.

4. BlackBerry systems used in the Army in Europe must be certified to meet the Federal Information Processing Standard (FIPS). FIPS certification protects unclassified Government information when leaving DOD-owned and -controlled networks. BlackBerry systems must use secure/multipurpose Internet mail extension (S/MIME) software to be Public Key Infrastructure (PKI) compliant. S/MIME-enhanced BlackBerry systems are subject to DOD, DA, and AE policy governing the security and use of unclassified information systems.

5. In addition to general security regulations and policy in the references, the following controls govern use of BlackBerry systems in the European theater:

a. The use of BlackBerry handheld devices must be included in the using organization's System Security Accreditation Agreement (SSAA). The Blackberry enterprise server (BES) must be included in the same SSAA as its host Microsoft exchange server.

b. The BlackBerry handheld device will not be used to process classified information (Confidential and above). If the device is compromised beyond the ability of the internal S/MIME "purging" features to ensure that no data remains or if the device is damaged beyond in-house repair capabilities, the device must be destroyed according to applicable Army regulations.

c. The BlackBerry handheld device will not be taken inside any permanent, temporary, or mobile sensitive compartmented information facility (SCIF) without approval of the senior official of the intelligence community (SOIC). Any infrared (IR) capability must be disabled before entering a SCIF. Although the device may be approved by the SOIC for use in a SCIF, the radio frequency (RF) capability will not be used. This restriction may be waived only by the Special Security Officer, Defense Intelligence Agency (DAC-2A), and only if use of RF capability in a SCIF is mission essential.

d. The BlackBerry handheld device will not be taken into areas where classified information is discussed or electronically processed except as provided for in subparagraph c above or AR 25-2, paragraph 4-28. Users will receive security-awareness training.

e. The BlackBerry handheld device will not be configured to work with or be connected to any device other than a Government-owned unclassified computer. Autoforwarding official mail (from a .mil e-mail address) to unofficial accounts (for example, a .com e-mail address) or unofficial devices is prohibited.

AEAIM-A
SUBJECT: BlackBerry Policy

f. The BlackBerry device will employ password protection for the device, the subscriber identity module (SIM) chip, and the handheld certificate store (handheld key store). Devices will be configured with a timeout of 30 minutes, a password history of three (3), and maximum password attempts of five (5). On the fifth failed attempt, all data on the device will be wiped automatically. Based on this password policy and the limitations of the device, passwords will be five alphanumeric characters with at least one alpha and one numeric character. BlackBerry passwords will be changed every 150 days.

g. Web-access and e-mail capabilities increase security risks, raise cell-phone costs, and reduce the quality of BlackBerry performance. BlackBerry devices will not be allowed to access the Web, and e-mail attachments will be blocked at the BES. The cell-phone policy in National Security Agency IDOC-002-03 (para 2c) applies to the “telephony capabilities” of the BlackBerry.

h. Every BES must comply with the latest Army in Europe BlackBerry policy (available from the USAREUR G6 (AEAIM-AP) (DSN 370-7724)). To reduce costs, BESs will be consolidated wherever technically feasible. BESs must have USAREUR G6 approval before being purchased or added to Army in Europe networks.

i. If a BlackBerry handheld device is lost or stolen, it must be reported immediately to the BES administrator. The BES administrator will immediately issue a “kill” command for the device, wiping all data from it.

6. BlackBerry devices are authorized for general officers, senior executive service (SES) civilian employees, promotable colonels, and for commanders and command sergeants major at the brigade level and above. Approval authority for all BlackBerry devices will be at the colonel (or civilian equivalent), HQ USAREUR/7A staff principal, or USAREUR major subordinate command commander level. This approval authority will not be delegated. Organizations and units subordinate to the IMA-E must request approval from the Director, IMA-E. Approval to purchase BlackBerry devices will be based on a valid requirement for mobile e-mail capability and granted only after considering the costs involved.

a. BlackBerry devices will be purchased with the necessary service as part of the USAREUR cell-phone contract at the requesting unit’s expense. No other contract source is authorized. Units are responsible for all costs for the device, licenses, monthly charges, and usage.

b. BlackBerry devices will be used only with the appropriate Common Access Card (CAC) sled. This will allow use of CAC certificates for PKI-enabled e-mail. Only the USAREUR G6 may approve requests for exception to this rule.

c. BlackBerry handheld devices must be maintained on installation and unit property books.

AEAIM-A
SUBJECT: BlackBerry Policy

d. Individuals are not authorized to have both a BlackBerry device and a cell phone unless the cell phone is a secure GSM mobile phone.

7. Unless specifically stated otherwise, only the DCG/CofS, USAREUR/7A, may approve exceptions to the policy in this memorandum.

8. The POC is Ms. Holland, DSN 370-3520, e-mail: karen.holland@us.army.mil.

FOR THE COMMANDER:



WILLIAM E. WARD
Lieutenant General, USA
Deputy Commanding General
Chief of Staff

DISTRIBUTION:
C (AEPUBS)