

CC POLICY MEMORANDUM #17
Protection of Information Technology (IT) Equipment and Sensitive Data

Original Document Date: 05/15/07

Revision Date: 08/05/09



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY CADET COMMAND
FORT MONROE, VIRGINIA 23651-5000

10 5 AUG 2009

ATAL-I

MEMORANDUM FOR All Personnel Assigned or Attached to U.S. Army
Cadet Command (USACC)

Subject: Policy Memorandum 17 - Protection of Information
Technology (IT) Equipment and Personally Identifiable Information
(PII)

1. References:

- a. Privacy Act, 5 U.S.C. 552a.
- b. Memorandum, Chief Information Officer (CIO)/G6, SAIS-GKP, 28 September 06, subject: Army Data-At-Rest (DAR) Protection Strategy
- c. HQ TRADOC, ATIM-T, 20 Sep 07, subject: Reporting the Loss of Personally Identifiable Information (PII)
- d. HQ TRADOC, ATIM-S, 31 Oct 06, subject: Guidance on Protecting Data-At-Rest (DAR)
- e. HQ TRADOC, ATIM, 30 May 07, subject: TRADOC policy Letter 16, Security of Government-owned or Leased Information Technology (IT) Equipment
- f. Memorandum, Director CIO/G6 Office of Information Assurance and Compliance, 18 Oct 06, subject: Implementation of Information Assurance Best Business Practice (IA BBP)

2. Purpose:

- a. To mitigate the loss of portable electronic devices (PEDs) and loss of Personally Identifiable Information (PII).
- b. To identify required actions for the loss of PEDs and loss or compromise of PII.

3. Scope. Provisions of this policy apply to all personnel assigned, attached to or working in support of USACC, including Junior ROTC Cadre.

CC POLICY MEMORANDUM #17
Protection of Information Technology (IT) Equipment and Sensitive Data

ATCC-I

- 5 AUG 2009

Subject: Policy Memorandum 17 - Protection of Information
Technology (IT) Equipment and Sensitive Data

4. The loss of a Personal Electronic Device (PED)s (including laptops, Blackberries and similar devices that store sensitive data) and removable media (CDs, DVDs, floppy disks, thumb drives, flash memory) that store personal data, has resulted in significant concern within the Federal Government. All personnel assigned to US Army Cadet Command (USACC) must ensure we are taking action to mitigate risk of the loss of equipment and sensitive data. Throughout the remainder of this policy, the term "PED" or "PEDs" also includes removable media.

5. Personal data which is considered reportable for Privacy Act purposes is quite extensive and includes Social Security Numbers (SSNs), marital status, mother's maiden name, date of birth, employment data, medical data, etc. Much of this data is required to initiate a request for security clearance (SF86) and may be captured and stored by the ROO on the ROO laptop or downloaded from USACC software applications to desktops. JROTC instructors are also reminded to avoid putting any Cadet personal data on their PCs or laptops.

6. **Required Actions.** To minimize the loss of PEDs and exposure of sensitive/personal data, the following actions are required by all personnel assigned, attached to, or working in support of US Army Cadet Command (USACC):

a. Minimize the storage of PII (personally identifiable information) on a PED. Delete any PII as soon as it is no longer needed.

b. PEDS shall not be left unattended and unsecured in the workplace. When in the office, if the device is not under one's immediate control, lock the device in the office, secure it with a locking cable mechanism, or place the device in an appropriate container (such as a safe, lockable closet or lockable cabinet). Ensure the entire JROTC or ROTC BN area is secured during non-business hours.

c. While traveling by POV or GOV, do not leave PEDs in the vehicle. The preferred method of security is for the traveler to hand carry the device/media and keep it in sight and within immediate reach at all times.

d. While traveling by airplane or train, PEDs must not be checked with other baggage. The preferred method of security is for the traveler to hand carry the PED onto the conveyance and carefully store and retrieve the PED from the overhead bin or under the seat. The PED must remain within the traveler's sight and within immediate reach at all times.

CC POLICY MEMORANDUM #17
Protection of Information Technology (IT) Equipment and Sensitive Data

- 5 AUG 2009

ATCC-I

Subject: Policy Memorandum 17 - Protection of Information
Technology (IT) Equipment and Sensitive Data

e. Report any lost or compromise of PII **IMMEDIATELY**. USACC must report to higher HQs within **1 HOUR** of suspected loss or compromise of PII.

f. Report any lost PEDs IAW USACC Policy Memorandum 9, Serious Incident Report, within 24 hours of discovering the loss. The report needs to include all details known about the loss and whether there was any sensitive data on the equipment. **Per paragraph 6a. above, loss of PII associated with the loss of equipment must be reported immediately.**

g. Do not give anyone your CAC pin or password for any systems you have access to. (e.g. CCIMS, JCIMS, USAAC portal, JROTC portal, or your PC/laptop)

h. Conduct regular vulnerability assessments of your physical security.

i. Your Information Assurance Security Officer (IASO) should do spot inspections of data on your unit's PEDs to ensure sensitive data is being stored in an approved, encrypted folder.

j. Ensure that you have anti-virus software installed on the equipment and the virus definition files are up to date. Make sure to run periodic scans or enable the auto scan feature. Ensure your software patches are up to date.

k. Ensure that you are storing any PII in an encrypted folder or with approved encryption software for the entire hard drive.

l. Do not install unauthorized software on government computers or laptops (i.e. Limewire, Frostwire, iTunes, etc.)

m. Secure all laptops with a cable lock that attaches the laptop via a key lock (no combination locks) to the desk or other immovable/hard to move object.

n. All PEDs will have a sticker on them approving them for travel, before they leave the unit. An USAAC Label 3 is affixed to the outside cover of the laptop computers so they will be visible for inspection, and a USAAC Label 2 will be used on the smaller portable devices, such as the Blackberry, thumb drives publications and forms re-supply channels who will order through the Supervisor of Publications and Forms, Information Services and other portable media. The labels will state that they comply with the Army data encryption standard and are authorized for

CC POLICY MEMORANDUM #17
Protection of Information Technology (IT) Equipment and Sensitive Data

ATCC-I

- 5 AUG 2009

Subject: Policy Memorandum 17 - Protection of Information
Technology (IT) Equipment and Sensitive Data

travel. The labels are available through your normal Division, Enterprise Services Branch, USAAC, Fort Knox, KY 4012 1, via DA Form 17, Requisition for Publications and Blank Forms

o. Each unit will maintain key control for the office/building, laptop cable locks, and all containers holding files with PII.

p. All USACC personnel will complete Information Assurance (IA) and PII on-line training annually or as required.

7. The above policy will be adhered to by all personnel assigned or attached to US Army Cadet Command (USACC). Leaders at each level of the command need to conduct regular vulnerability and property control inspections to ensure we protect our equipment and sensitive data. The unit IASO will conduct checks on unit IT equipment to ensure sensitive data isn't being stored outside of encrypted folders/hard drives. Commanders, at all levels, are responsible for this policy being read, understood, and complied with by all personnel in their unit.

8. Military personnel may be subject to disciplinary action and civilian employees may be subject to adverse personnel action for violations of this policy.



ARTHUR M. BARTELL
Major General, U.S. Army
Commanding General