



UNITED STATES MARINE CORPS
2D MARINE AIRCRAFT WING
II MARINE EXPEDITIONARY FORCE
POSTAL SERVICE CENTER BOX 8050
CHERRY POINT, NC 28533-0050

IN REPLY REFER TO:
2000
G-6
19 AUG 2010

Policy Letter 09-10

From: Commanding General, 2d Marine Aircraft Wing
To: Distribution List

Subj: 2D MARINE AIRCRAFT WING (2D MAW) POLICY LETTER ON
PERSONALLY IDENTIFIABLE INFORMATION

Ref: (a) Marine Corps Enterprise Information Assurance
Directive 011
(b) DISA Personally Identifiable Information Training
(c) DON CIO msg dtd 181430Z MAY 09 Department of the Navy
Privacy Impact Assessment (PIA) Guidance
(d) MCI East msg dtd 261346Z Use and Safeguard of
Personally Identifiable Information in messages and
E-mails

1. Situation. This policy letter provides guidance on the implementation of the references in order to ensure compliance while preventing the disclosure of Personally Identifiable Information (PII).

2. Cancellation. Policy Letter 05-09.

2. Mission. To ensure PII is properly handled and preventable steps are practiced to prevent the unauthorized disclosure of PII in 2d MAW.

3. Execution

a. Commander's Intent. Reinforce Department of Defense and USMC policies on the handling, storage and receipt/transfer of PII and take aggressive action toward preventing the unauthorized disclosure of PII.

b. Concept of Operations. In order to prevent unauthorized disclosure of PII all personnel must be familiar with the methods and practices in safeguarding PII. This policy letter provides guidance to decrease PII security incidents and inform 2d MAW personnel on PII protection practices.

DISTRIBUTION STATEMENT A: Approved for public release;
distribution is unlimited.

Subj: 2D MARINE AIRCRAFT WING POLICY LETTER ON PERSONALLY IDENTIFIABLE INFORMATION

c. Tasks

(1) AC/S, G-6

(a) Provide technical assistance as required to identify PII on shared drive.

(b) Conduct shared drive scans to indentify PII stored that is not in compliance with DoD and Marine Corps policy.

(c) Coordinate 2d MAW reporting requirements in accordance with the references.

(d) Provide support for PII training requirements.

(2) Department Heads and Group Commanders

(a) Designate lead in removing/modifying PII information on public information repositories.

(b) Ensure personnel follow guidelines on the storage and distribution of PII in your organizations.

(c) Coordinate efforts of all subordinate squadrons under your administrative control.

d. Coordinating Instructions

(1) Review unit/section public information repositories (share drives, SharePoint Portal, etc.) to ensure PII is stored in accordance with this policy.

(2) Remove all files (documents, spreadsheets, databases, etc.) containing PII that are no longer required.

(3) Files containing PII that are required will be modified to be password protected.

(4) Files containing PII that are emailed will be password protected and the email itself will be encrypted.

(5) Naval messages and E-mails containing PII will be digitally signed and encrypted.

(6) A PII breach must be reported immediately to the 2d MAW G-6 Information Assurance Manager during working hours or 2d MAW CDO during non working hours. A breach of PII occurs when PII is lost, stolen, released without proper need, improperly

Subj: 2D MARINE AIRCRAFT WING POLICY LETTER ON PERSONALLY IDENTIFIABLE INFORMATION

distributed, or incorrectly disposed. A breach is defined as an actual or possible loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic where one or more individuals could be adversely affected. The following scenarios are examples of PII breaches:

(a) A recruiter has just completed an enlistment package and goes to lunch. He leaves his laptop in his vehicle and enters the establishment to eat. Upon returning, he discovers the car has been broken into and the laptop stolen. The enlistment information collected on the ONE recruit stored on the laptop is considered as a PII breach and must be reported.

(b) An officer loads his command's fitness reports onto a thumb drive to work on over the weekend. On his way to the car, the thumb drive falls out of his pocket and is lost. The officer's command consists of over 300 Marines. Upon realizing it was lost, the officer retraces his steps and finds the thumb drive two days later. Despite finding the thumb drive, the data was in an uncontrolled environment. This is a PII breach and must be reported.

(c) A backup tape of a large database that holds payroll information is unaccounted for. A search for the tape turns up evidence that a former employee stole the tape. The tape contains information on over 15,000 Marines. This is a PII breach and must be reported.

(d) An unencrypted email containing PII is sent to a group of Watch Officers who have a business-need to view the information. This is a PII breach and must be reported.

(e) An encrypted email containing PII is sent to a group of Watch Officers who do not have a business-need to view the information. This is a PII breach and must be reported.

(7) All personnel complete annual PII training on an annual basis NLT than the last day of the last month each calendar year via MarineNet or <http://iase.disa.mil/eta/>.

(8) All personnel complete annual Information Assurance Training on an annual basis NLT than the last day of the last month each calendar year via MarineNet or <http://iase.disa.mil/eta/>.

Subj: 2D MARINE AIRCRAFT WING POLICY LETTER ON PERSONALLY
IDENTIFIABLE INFORMATION

4. Administration and Logistics. Points of contact are the AC/S
G-6 (IAM) at DSN 582-2366 or AC/S, G-6 IA Section at DSN 582-
7506.

5. Command and Signal

a. Command. This Policy Letter is applicable to all 2d MAW
units.

b. Signal. This Policy Letter is effective date signed.


J. M. DAVIS

DISTRIBUTION: A