NATIONAL HEADQUARTERS CIVIL AIR PATROL

CAP REGULATION 1-2

3 APRIL 2012

Corporate Principles

PERSONALLY IDENTIFIABLE INFORMATION

This regulation defines rules for protecting Personally Identifiable Information (PII), collected, generated, or maintained by Civil Air Patrol (CAP), from unauthorized disclosure and emphasizes the role of CAP users in ensuring that the appropriate physical and technical safeguards are in place to protect all CAP systems (both hard copy and electronic) that contain PII. This regulation applies to all CAP members.

1. General. Personally identifiable information (PII) is CAP confidential information about an individual that can be used to distinguish or trace that individual's identity. Examples of PII include, but are not limited to, social security number; age; marital status; race; date and place of birth; telephone numbers; other demographic, medical history, personal, medical and financial information. Unauthorized access to the PII of members/employees must be prevented to the maximum extent possible. PII shall only be made available to those individuals who have a specific need to have such information and shall be provided for official CAP business only.

2. Responsibilities.

a. Commanders/Directors.

(1) Only require the collection of personal information that is absolutely necessary to conduct CAP business (see paragraph 3a below).

(2) Ensure that all personnel within their area of responsibility understand the need to protect PII.

b. Members. Protect PII that has come into their possession during the normal conduct of CAP business IAW paragraph 3b below.

3. Protection.

a. Limit the use of PII to absolute need. Whenever possible, forms, applications and other documents should use only the individual's name, CAP grade and CAPID. Additional information about the individual may then be drawn from the online personnel database, which has appropriate security measures.

b. Limit access to PII that has been acquired as part of normal CAP processes. Personal discipline on the part of the custodian of CAP records/documents containing PII is key to preventing unauthorized access.

OPR: EXS

Distribution: National CAP website. Pages: 2

(1) CAP records/documents containing PII must be kept under lock and key or in a secure electronic file that is password protected when the records/documents are not in use.

(2) When leaving your work area, records containing PII must not be left open and unattended, or in any manner that would allow the data to be seen by an unauthorized individual.

(3) Do not leave unattended any laptops, tablet PCs, smartphones, USB flash drives or personal digital assistants (PDA) containing PII.

(4) Delete any data containing PII as soon as practical after completing the tasking for which the PII data was acquired.

(5) CAP publications and forms issued by any level of command that include requirements to collect or use PII must contain instructions for protecting PII.

(6) All devices containing PII should be password-enabled or have data encryption standards installed (if possible) to prevent unauthorized access to the data if the device is stolen or lost.

(7) If PII is to be transmitted via radio, only the absolute minimum amount of information essential to mission accomplishment should be transmitted using encrypted radio transmissions if possible.

4. Disposal. Disposal methods are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

a. Examples of disposal methods for paper records include, but are not limited to tearing, burning, shredding, or mutilation.

b. Examples of disposal methods for electronic records and media include, but are not limited to, overwriting, degaussing, disintegration, pulverization, burning, shredding or sanding. Just deleting electronic files containing PII is not sufficient.

5. What to do in the case of a Breach. If a CAP member becomes aware that his/her or another member's PII may have been released, that member will notify his/her commander as soon as feasible. The commander is responsible for ensuring that the member(s) whose information may have been released or disclosed is notified of that release of information, to include the specific PII that may have been released. If a single incident results in the release or disclosure of PII of 10 or more members, the commander will notify the National Headquarters General Counsel's office (NHQ/GC) of the name and CAPID of the member(s) whose information may have been released, with an information copy of the notification to the group, wing and region commander (as appropriate). Individual wings need to consult with their legal officers to assure compliance with state standards, if any.

CHARLES L. CARR, JR.
Major General, CAP
Commander