NATIONAL HEADQUARTERS CIVIL AIR PATROL

CAP REGULATION 110-1

27 DECEMBER 2012

Information Technology

CAP ELECTRONIC SYSTEMS AND DATA ADMINISTRATION

This regulation establishes policies and procedures for the management of Civil Air Patrol (CAP) electronic information, communication and data systems including, but not limited to servers, network systems, personal computers, software applications, websites, web applications and data files. This regulation is applicable to all CAP units and volunteer National staff.

SUMMARY OF CHANGES.
Purpose of the regulation is revised; definition of CAP Internet and Local Computer Operations has been expanded; password selection criteria have been added; requirements for securing personally identifiable information (PII) have been added; additional prohibited CAP internet operations have been established; requirement for annual unit website review has been added; prohibition of release of Public Affairs Information without PAO approval has been added; anti-virus protection requirement for all CAP computers has been added. **Note: This regulation is revised in its entirety.**

1. General. The purpose of this regulation is to ensure the security and integrity of CAP corporate and member information and data, and to ensure the presentation of a positive image of CAP via the worldwide web.

2. CAP Domain Operations are defined as any activity operated or conducted through the internet which makes use of a domain name that uses the name "Civil Air Patrol", its insignia, copyrights, emblems, badges, descriptive or designating marks or words used in carrying out the Civil Air Patrol program. Civil Air Patrol's names and marks are specifically owned by Civil Air Patrol pursuant to 36 United States Code § 40306.

3. Operations in .gov domains must follow all applicable policies and guidelines specified for the domain in addition to the requirements of this regulation. Policies regulating the .gov domain may be found online at http://ns1.cap.gov/. All links on CAP.gov websites to services in other domains must include a statement or pop-up window stating that the user is leaving the .gov domain or being redirected to a non .gov site.

4. CAP.gov Administrator (CGA) is a CAP member appointed by the National Commander (CAP/CC) who is responsible for the management of the CAP.gov internet domain. A new CGA may be appointed at any time. The CGA's duties are to:

a. Serve as the administrative contact for CAP.gov with the General Services Administration (GSA).

b. Serve as the primary technical and billing contact with the GSA.

Supersedes: CAPR 110-1, 1 January 2000. OPR: IT
Distribution: National CAP website. Pages: 4

c. Establish the domain name server network for CAP.gov.

d. Implement policies for the orderly use of CAP.gov zone delegations in service to all echelons of CAP units.

e. Appoint, with the approval of the CAP/CC, other CAP members to act as assistants to the CGA.

5. CAPNHQ.gov Administrator is the CAP NHQ employee who:

a. Serves as the administrative, technical and billing contact for CAPNHQ.gov with the GSA.

b. Establishes the domain name server network for CAPNHQ.gov.

c. Implements policies for the orderly use of CAPNHQ.gov, capmembers.com and gocivilairpatrol.com zone delegations in service to National Headquarters and such CAP echelons as directed by the Chief Operating Officer (NHQ/CO).

6. CAP Internet and Local Computer Operations are data, communication and information operations that utilize the internet for hosting CAP websites, file services, e-mail, instant messaging and other communications and sharing vehicles. Local computer operations include CAP-owned personal computers, smartphones, tablet PCs and external storage devices that contain CAP data and information.

7. Password Selection Criteria. Choosing a strong password is an important part of protecting your website access. Create passwords that can be easily remembered, but not easily figured out by potential intruders.

- Passwords chosen must
  - be a minimum of eight (8) characters in length
  - be memorized; if a password is written down it must be secure
  - contain at least one character from three of the following categories:
  - Uppercase letter (A-Z)
  - Lowercase letter (a-z)
  - Digit (0-9)
  - Special character (~`!@#$%^&*()+=_-{}[]\|:;”’?/<>,.)

- Passwords chosen must not
  - contain a common proper name, login ID, e-mail address, initials, first, middle or last name

If you suspect your password has been compromised make every effort to change it immediately. For more recommendations on Online Privacy and Safety, please visit http://www.microsoft.com/security/online-privacy/passwords-create.aspx.

8. Securing Personally Identifiable Information (PII). CAP policies governing the storage, use and security of PII are found in CAPR 1-2. When PII is placed on a web server or local computer, reasonable security, such as password access, must be implemented to protect the information.

a. CAP units that collect and transmit PII must take the proper steps to ensure data transmissions are protected. Secure Socket Layers (SSL), a protocol for encrypting information over the Internet and/or secure websites are recommended practices in encrypting PII data transmissions. Data and database access must be controlled by at least a login. Operating databases on a public-facing server, such as a Web server, is not recommended.

b. Anytime PII is transmitted by the internet it shall be accompanied by the following notice:

"Warning: The information you are receiving is protected from interception or disclosure. Any person who intentionally intercepts or illegally uses, distributes, reproduces or discloses its contents is subject to the penalties set forth in 18 United States Code Section 2511 and/or related state and federal laws of the United States."

9. Prohibited CAP Internet Operations. The following are prohibited internet operations:

a. Recording or transmitting social security numbers (SSN) on field developed applications (including last four digits of SSNs).

b. Creation or distribution of any disruptive or offensive messages such as pornography or offensive comments about race, gender, appearance, disabilities, age, sexual orientation, religious beliefs or practice, political beliefs, national origin or disabilities.

c. Creation or distribution of any language or material that is obscene, indecent, offensive, defamatory, abusive, harassing, disrespectful or hateful.

d. Communication that invades privacy or encourages conduct that would constitute a criminal offense, give rise to civil liability or that otherwise violates any local, state, national or international law or regulation.

e. Use or distribution of any unsolicited or unauthorized advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes" or any other form of solicitation.

f. Advertising on any .gov domain. For the purposes of this section, "advertising" shall not include the recognition of individuals or companies that have demonstrated financial or other support to the performance of CAP missions. When such recognition is extended via links or references to non-CAP sites, a disclaimer, in no less than 8-point type, shall be clearly displayed stating:

"LINKS OR REFERENCES TO INDIVIDUALS OR COMPANIES DO NOT CONSTITUTE AN ENDORSEMENT OF ANY INFORMATION, PRODUCT OR SERVICE YOU MAY RECEIVE FROM SUCH SOURCES."

g. Communication that contains false statements about Civil Air Patrol or Civil Air Patrol employees or members.

h. Publication or distribution of any information that violates any copyright, trade name or trademark.

10. Enforcement. Civil Air Patrol reserves the right, but undertakes no duty of a continuous monitoring of communications or systems in order to enforce the provisions of this regulation. Such enforcement if undertaken may, however, involve National Headquarters and/or appropriate unit, group, wing or region commanders in

a. resolving the matter informally; and/or

b. initiating disciplinary proceedings; and/or

c. withdrawing approval for a particular CAP internet operation; and/or

d. limiting access to a CAP internet operation to CAP members; and/or

e. for a prohibited CAP internet operation conducted on equipment or a domain outside of CAP's immediate control, referring the matter to CAP/GC to recommend informal, formal and/or legal action to be taken (i.e., possible filing of civil action or referral to federal, state, tribal or local law enforecement authorities).

11. Approval to Conduct CAP Internet Operation.

a. CAP units conducting CAP internet operations (including cap.gov domains) must obtain and maintain a record of approval from the CAP/CC or applicable region, wing commander or their designee. The NHQ/CO or designee approves CAPNHQ.gov domain delegations.

b. Request for CAP.gov or CAP.US domain services can be located on http://ns1.cap.gov/

c. A listing of all approved domain names and websites will be maintained in eServices and will include the URL, webmaster, unit commander, date of approval and date of latest review. Reviews shall be conducted and re-approval documented prior to 30 September each year. All units will provide their respective wing headquarters with the login credentials and hosting information to their websites to ensure a continuity plan exists. If the webmaster should leave, someone should be able to take over duties easily.

d. The approval or review of CAP subordinate unit websites can be submitted by using the internet operations application located in eServices.

12. Withdrawal of Approval. Approval to conduct internet operations for CAP.gov domain delegations or other CAP internet operations may be withdrawn, at any time, by the CAP/CC, the appropriate region or wing commander or their designee. Approval to conduct internet operations for CAPNHQ.gov domain delegations may be withdrawn, at any time, by the NHQ/CO or designee.

13. Identification. CAP operations involving web pages must contain the name "Civil Air Patrol" and clearly identify the name of the sponsoring unit on the main page of the site. CAP operations involving e-mail, chat groups, bulletin boards, list-servers or similar communications must include the name of the person involved in the communication and, as applicable, their CAP grade or CAP duty position.

14. Public Affairs Information. CAP members shall not use CAP internet operations to disseminate information that would normally be distributed through public affairs officers without commander or the releasing PAO's approval.

15. Information Protection. Anti-virus protection shall be operational on all CAP computers. Free anti-virus software is available through eServices for CAP corporate computers. Regular backup of websites and applications is strongly recommended. CAP files maintained on CAP computers will be backed up in accordance with CAPR 10-2, *Files Maintenance and Records Disposition*.

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