OFFICE OF THE NATIONAL COMMANDER
NATIONAL HEADQUARTERS
CIVIL AIR PATROL
UNITED STATES AIR FORCE AUXILIARY
MAXWELL AIR FORCE BASE, ALABAMA 36112-5937

18 July 2019

MEMORANDUM FOR ALL CAP MEMBERS

FROM: CAP/CC

SUBJECT: Interim Change Letter – CAPR 120-1, *Information Technology Security,* 1 October 2017

1. Since the release of CAPR 120-1, additional security measures have been identified as necessary to enhance protection of Civil Air Patrol's information systems. The focus of these changes is centered on preventing circumvention of eServices authentication as well as added data protection requirements.

2. eServices authentication is in place to ensure system integrity by restricting access to authorized end users. Risk to our systems occurs when tools, such as automated scripting or bots, are used to logon to eServices from external systems. In doing so, members risk collection, however temporary, of their account information by these systems making unauthorized use of their account possible. Individuals who develop and provide information technology applications that employ these prohibited services place all CAP data at risk.

3. Recent international and federal data protection regulations have emphasized the need for diligence in the security of our members' data. To reduce Civil Air Patrol's jurisdictional and security risk, General Counsel and the CIO/DCIO have determined that all Civil Air Patrol data must be hosted within the continental United States.

4. This interim change letter will remain in effect until the next revision.

5. CAPR 120-1 is amended as follows.

a. Paragraph 6 Unacceptable Use. Change subparagraph 6.16. to read:

6.16. Members may not attempt to circumvent the eServices authentication or security of any account, network, or host. This will include, but is not limited to:

- accessing an account or data for which the member is not authorized outside of their eServices permissions or approved CAPWATCH dataset.
- probing the security of the networks.
- attempting an unauthorized upload or change to information in eServices.
- as a member who creates or manages local information technology, using automated scripting tools that circumvent the user's eServices logon within the local application.
- as a member who uses local applications, providing your eServices account information for use by a local application or service utilizing automated scripting tools that circumvent the eServices end user logon. When members need to access eServices applications, they must logon through the NHQ IT eServices

logon page and not through any local application or service. Local applications and/or services that logon to eServices on behalf of the member are not permitted and will not be used by members.

b. Paragraph 11 Data Security. Add subparagraph 11.8. to read:

11.8. When selecting commercial cloud services, IT Directors and IT Officers must ensure that the service is hosted inside the boundaries of the United States to avoid jurisdiction issues and concerns about inadequate security controls.

6. Please direct any questions you might have to capadmin@capnhq.gov.

Mark E Smith

MARK E. SMITH
Major General, CAP

NATIONAL HEADQUARTERS CIVIL AIR PATROL

CAP REGULATION 120-1

1 OCTOBER 2017

Information Technology

INFORMATION TECHNOLOGY SECURITY

This regulation establishes policies and procedures for the management of Civil Air Patrol (CAP) electronic information and data systems including, but not limited to, servers, computer network systems, personal computers, software applications, websites, web applications and data files. Responsibilities for management and use of CAP radio networks is not within the scope CAPR 120-1. This regulation is applicable to all CAP units and members.

SUMMARY OF CHANGES.

This regulation supersedes CAPR 110-1 *CAP Electronic Systems and Data Administration*. It has been extensively revised and needs to be reviewed in its entirety. In some cases, existing requirements have been reorganized into common categories for the purpose of clarity. There are also additional security considerations defined within the regulation, such as connecting mobile/smart devices to unsecured networks, and others strengthened, such as the policy related to reporting security incidents.

TABLE OF CONTENTS.

1. Purpose.

1.1. The purpose of this regulation is to ensure the security and integrity of CAP information systems and data. This policy applies to all CAP members who have access to CAP Information Technology (IT) assets, computer networks and corporate data and must be followed whether using CAP-owned IT assets or personal assets in the conduct of CAP business. Effective security is a team effort involving the

participation and support of every CAP member who deals with information and/or information systems. Every computer and smart device user is responsible to know these guidelines, and to conduct his/her activities accordingly.

2. Definitions, Roles and Responsibilities.

2.1. Definitions.

2.1.1. CAP resources are defined as any hardware, software or computer network access that is provided by the Civil Air Patrol. Where responsibilities arise to protect CAP computer networks and data accessed via personally owned computing resources, including but not limited to smart phones, laptops and tablets, those responsibilities will be called out specifically.

2.1.2. 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.

2.1.3. CAP Internet Operations are defined as data, communication and information operations that utilize the internet for hosting CAP websites on a CAP.gov domain, including file services, e-mail, instant messaging and other communications and sharing vehicles.

2.1.4. Local Computer Operations include any activity using CAP-owned computers, tablets and external storage devices as well as personally owned devices used to conduct CAP business.

2.1.5. Field developed applications are IT systems including but not limited to websites, databases, and applications that are developed by and offered to units outside IT systems provided by NHQ.

2.2. Roles and Responsibilities.

2.2.1. The Civil Air Patrol, National Commander (CAP/CC) is responsible for approving and removing CAP Internet Operations.

2.2.2. The Civil Air Patrol Chief Operating Officer (COO) is responsible for approving and removing CAPNHQ.gov domain delegations.

2.2.3. The Chief Information Officer (CIO) has overall responsibility for the administration of IT programs for Civil Air Patrol.

2.2.4. The NHQ Deputy Director for IT, is responsible for assisting in the administration of IT programs for Civil Air Patrol and serves as the CAP.gov Administrator (CGA) responsible for the management of the CAP.gov internet domain. The CGA's duties are to:

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

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

2.2.4.3. Establish the domain name server network and email administration for CAP.gov.

2.2.4.4. Implement policies for the orderly use of CAP.gov zone delegations in support of all echelons of CAP units.

2.2.4.5. Implement policies for the orderly use of CAPNHQ.gov, capmembers.com, gocivilairpatrol.com and other National Headquarters Corporate website zone delegations in service to National Headquarters and such CAP echelons as directed by the Chief Operating Officer (CAP/COO).

2.2.5. Wing and Region Directors of IT and subordinate or assistant IT Officers in the field are responsible for maintenance, upkeep and compliance with regard to use of all CAP IT assets within their respective units in accordance with local and applicable CAP policy. Where IT Officer billets are filled in subordinate units, responsibility can be delegated to its lowest reasonable level. They also ensure that administration of Region and subordinate domains are managed in accordance with Region or Wing procedures. Wings and Regions must either appoint a Director of IT or ensure that someone within their organization is accountable for IT responsibilities described within this regulation.

2.2.6. Web Security Administrators (WSA) are responsible for managing permissions to eServices applications for their unit.

3. Operating Instructions (OI), Pamphlets, Supplements and Waivers to this Regulation.

CAP/CIO is the approval authority for all OIs, pamphlets, and supplements to this regulation. OIs, pamphlets and supplements to the regulation cannot be issued below the wing level. Requests must be coordinated through the wing and region commanders and will be reviewed for approval by the CAP/CIO or designee.

CAP/CIO is the approval authority for waivers to this regulation. Requests must be coordinated through the wing and region commanders and will be reviewed for approval by the CAP/CIO or designee.

4. Monitoring and Privacy.

4.1. CAP reserves the right to monitor and/or log all CAP Internet Operations with or without notice, including CAP.gov email and all website communications, and therefore, members will have no reasonable expectation of privacy in the use of these resources.

4.2. Refer to paragraph 13.1 "Proper Use of CAP Email Systems" for monitoring related to CAP.gov email accounts.

5. Acceptable Use.

5.1. CAP's computing resources shall only be used for conducting/accomplishing CAP business. All other use is prohibited.

5.2. Conducting Approved CAP Internet Operations.

5.2.1. CAP units conducting CAP Internet Operations (including CAP.gov domains) must obtain and maintain a record of approval from the next higher commander. The CAP/COO or designee approves CAPNHQ.gov domain delegations. Requests for CAP.gov or CAP.US domain services must be submitted through eServices to the CAP.gov Administrator (http://ns1.cap.gov/). This requirement does not apply to website requests to support national level activities. In those instances, the request must be submitted to NHQ OPR for approval and establishment of website by NHQ IT.

5.2.2. A listing of all approved domain names and websites will be maintained in eServices on the Internet Operations Approval page and will include the URL, webmaster, unit commander, date of approval and date of latest review. The NHQ Deputy Director for IT is responsible for managing the list of approved domain names and websites. Commanders, or their designees, shall review and document re-approvals prior to 30 September each year. All units will provide their respective wing headquarters with login credentials and hosting information to their websites to ensure continuity plan in the case of personnel changes. In the event that the login credentials change during the year, commanders or their designees are responsible for submitting those changes to the Internet Operations record. This information may only be submitted through the eServices application; email submissions will not be accepted.

5.2.3. 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 pages which contain 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. The approval or review of CAP subordinate unit websites must be submitted by using the Internet Operations application located in eServices.

5.2.4. 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 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 CAP/COO or designee. Notices of withdrawal of approval are normally sent via email. There is no appeal process.

5.3. 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 and/or CAP duty position.

5.4. 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. While CAP-owned resources may be used in the course of conducting public affairs, guidelines for those activities are provided in CAPR 190-1, *Civil Air Patrol Public Affairs Program*.

6. Unacceptable Use.

6.1. Users may not download any software or download/upload files via the internet, using either a CAP-owned or personal asset conducting CAP business, in ways that are inconsistent with their licenses or copyrights.

6.2. Knowingly displaying any kind of sexually explicit image or document on any CAP system will not be tolerated. In addition, sexually explicit material shall not be archived, stored, distributed, edited or recorded using CAP computing resources. If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately. If you receive an unsolicited inappropriate email, you must report it to the unit IT Officer and delete it.

6.3. CAP's computing resources, whether operating on a CAP-owned or non-CAP owned network, must not be used knowingly to violate the laws and regulations of the United States or the laws and regulations of any state, city or other local jurisdiction in any material way. Use of any CAP resources for illegal activity is grounds for disciplinary action, up to and including termination of membership. Additionally, CAP will cooperate with any legitimate law enforcement agency.

6.4. Postings by members from a CAP e-mail address to newsgroups are not permitted except in the course of business duties.

6.5. Recording or transmitting social security numbers (SSN) on field developed applications (including last four digits of SSNs) is not permitted.

6.6. Creating or distributing any electronic message that is determined by command staff to be disruptive or offensive such as pornography or offensive comments about race, gender, disabilities, age, sexual orientation, religious beliefs or practice, national origin or disabilities.

6.7. Creation or distribution of any language or material that is obscene, indecent, offensive, defamatory, abusive, harassing, disrespectful or hateful is not permitted.

6.8. Use or distribution of any unsolicited or unauthorized advertising, promotional materials, “junk mail,” “spam,” “chain letters,” “pyramid schemes” or any other form of solicitation is not permitted. This includes making fraudulent offers of products, items, or services.

6.9. Advertising or fundraising on any .gov domain is not permitted. For the purposes of this section, "advertising" does 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.”

6.10. Users will not use CAP computing resources to knowingly communicate false statements about Civil Air Patrol or Civil Air Patrol employees or members.

6.11. Unlawful copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, videos and the installation of any copyrighted software for which CAP or the end user does not have an active license is strictly prohibited.

6.12. Under no circumstances is anyone utilizing a CAP-owned IT asset authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CAP –owned or –licensed resources.

6.13. Intentional introduction of malicious programs into the network or server (e.g., viruses, spyware/malware, worms, Trojan Horses, e-mail bombs, etc.) is not permitted.

6.14. Revealing your account password to others or allowing use of your account by others. This includes family, household members or other CAP members. In some cases, members will require assistance of their IT Officer to address hardware/software issues which is impeding their ability to conduct CAP business. In these cases, members may share account information for the express purpose of remediating the issue. IT Officers will treat such information with care and only use it in the course of assisting the member with the identified issue.

6.15. Users will not knowingly cause security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data for which the member is not an intended recipient or logging into a server or account that the member is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, use of password breaking software, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

6.16. Members may not attempt to circumvent the system authentication or security of any account, network, or host. Please note that this would include, but is not limited to, accessing an account or data for which the member is not authorized, probing the security of the networks or attempting an unauthorized upload or change to information on eServices.

6.17. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a member's session, via any means, locally or via the internet/intranet is not permitted.

6.18. Providing unauthorized information about, or lists of, CAP personnel to parties outside CAP is not permitted unless required in the course of CAP business. This exception would include instances such as communication with USAF and other CAP partners that are necessary to execute the CAP mission.

6.19. Users may not install any software that does not facilitate execution of the CAP mission, whether from a purchased or download source, to any computer or related equipment/device that is furnished to the user by Civil Air Patrol.

7. Responsible Computer and Network Use.

7.1. Portable data storage devices (external hard drives, memory sticks, CD-RW disks, etc.) present a significant risk of transporting viruses, worms, etc., between computers. Files received from outside sources shall be virus scanned using the available anti-virus scanner software provided on CAP computers prior to opening a file if it cannot be verified as from a trusted source. All portable storage devices acquired for or on behalf of CAP are CAP property. Each member with either a CAP-owned device or a personally-owned device that contains CAP data is responsible for the security of that device. Members must avoid leaving devices unattended (i.e., an automobile, airports, hotel rooms, and restrooms).

7.2. Members who have CAP-owned data stored on their computer must not connect to any unsecured network ***without*** up-to-date software firewall and antivirus/anti-malware application configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from an unprotected home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the organization.

7.3. It is strongly recommended that members always connect to a password protected wireless network. Users shall pay particular attention when connecting to public hotspots, to ensure that they are connecting to the intended wireless access point, and not a mobile hotspot set up for malicious purposes.

7.4. Any member accessing their CAP.gov email account shall scan file or document attachments received from unknown senders for viruses, using the available corporate anti-virus scanner, located on eServices. Attachments may contain viruses, spyware, e-mail bombs, or Trojan horse code that could impose risk to CAP systems.

8. Password Policy

8.1. IT Officers are responsible for setting password policies for local field developed applications/systems that ensure that user access is controlled and restricted to authorized users. Password policies must reasonably align with accepted business standards.

8.2. Keep passwords secure and do not share accounts. Users must memorize their password(s) or store them in secure commercially available password manager applications. DO NOT place passwords

on desks, walls, sides of terminals, store them in a function key, login scripts, or any other communication software. If a password is compromised as a result of negligence or ignorance, members are accountable for any activity attributed to their account.

8.3. It is required that members do not use the same password on multiple corporate accounts.

8.4. Members should prevent anyone from observing as they enter a password.

8.5. If a password needs to be reset, proper identification may be required.

8.6. The NHQ IT Department will never ask for a member's password. If it is necessary to reset the password to a member's account for troubleshooting, NHQ will assign a new password to the account. Upon first login after the troubleshooting is complete, the user will be forced to enter a new password.

8.7. Members must not allow others to use their account after login is accomplished.

8.8. If others in the member's unit require additional access to do their assigned job, a request for access shall be made to through the Commander and unit WSA. A requirement for access to system(s) that has not yet been provided is not a valid reason for sharing accounts or passwords.

8.9. Authorized users are responsible for the security of their passwords and accounts.

8.10. User level passwords shall be changed at least every 180 days.

8.11. If a members suspects their password has been compromised, the member must notify the NHQ Deputy Director for IT and make every effort to change it immediately.

9. Confidential Data.

9.1. Confidential data is often the data that holds the most value to CAP. Because this type of data is also valuable to others outside the organization, often for nefarious purposes, it is important to safeguard CAP's confidential data. While the following list is not exhaustive, it contains some of the most common types of confidential data that shall be protected.

- Financial data which has not been released publicly
- Network diagrams and security configurations
- Communications about organization legal matters
- Mishap related information
- Complaints filed with an inspector general
- Credit card information/cardholder data
- User names and passwords
- Bank account information and routing numbers
- Payroll information
- Any confidential data held for a third party
- Member government issued identification numbers such as social security numbers, or other personal non-public information
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)

9.2. All members with access to confidential data shall take reasonable steps to protect it. This includes clearing the "downloads" folder of any downloaded reports containing confidential information

regularly. Responsibilities described under various sections of this policy, including mobile/smart devices, password and remote access guidance, etc. are all designed to protect CAP data. A subset of confidential data falls into the class of Personally Identifiable Information (PII). CAP policies governing the storage, use and security of PII are found in CAPR 1-2 (I); however this section defines additional guidance related to collection, transmission or display of electronic PII.

9.2.1. When PII is placed on a web server or local computer, reasonable security, such as password access, must be implemented to protect the information. Access shall be granted by permission/invitation. Local administrators are responsible for deleting access for users who are no longer with CAP or otherwise no longer have a business need for access.

9.2.2. Any external storage device containing PII, must be password protected.

9.2.3. CAP units that collect and transmit PII must take the proper steps to ensure data transmissions are protected. Members are required to use encryption protocols that reasonably align with accepted business standards for encrypting PII data transmissions. Data and database access must be controlled by at least a login. Operating a non-authenticating database on a public-facing server, such as a Web server, is not permitted.

9.2.4. Internet pages dealing with confidential information will be clearly marked/labeled. Members shall take all reasonable steps to prevent unauthorized access to this information. Anytime PII, (other than SSN data which is prohibited) 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."

10. Mobile Device.

10.1. Laptops.

10.1.1. CAP-Owned.

10.1.1.1. All laptops acquired for or on behalf of CAP are CAP property. Each member issued a laptop is responsible for the security of that laptop, regardless of whether the laptop is used in the office, at the member's place of residence, or in any other location such as a hotel, conference room, car, or airport. Members must avoid leaving their laptop unattended and should use hotel room safes, where available, to store unattended laptops when on business travel. Under no circumstances are members allowed to check their laptop in with luggage or check laptops in at planeside. In the event that the Department of Homeland Security (DHS) issues guidance prohibiting laptops as carry-on items aboard commercial aircraft, DHS regulations will apply. Use common sense to prevent laptop theft. Members could be held responsible if their laptop is missing, lost or stolen in accordance with CAPR 174-1, *Property Management and Accountability*.

10.1.1.2. Laptops that have to be temporarily left unattended must be placed in the secure location and secured with a security device if available. Laptops not used for several days or longer must be locked out of sight in a secure place.

10.1.1.3. All new CAP-owned laptops issued must be equipped with full-disk encryption. Encryption of existing laptops is at the discretion of unit IT Officer.

10.2. Mobile/Smart Devices.

10.2.1. All users of mobile/smart devices must use reasonable physical security measures. Members who have CAP-owned data on their personally-owned devices are expected to secure them whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices. This is especially important whenever personally-owned devices contain corporate data.

11. Data Security.

11.1. Confidential data must not be stored on mobile/smart devices unless required for a defined business need.

11.2. Passwords and other confidential data are not to be stored unencrypted on any CAP device or personally-owned device containing CAP data.

11.3. CAP data stored on personally owned mobile/smart devices must be securely disposed of using methods such as physical destruction (if the device is not to be used again), the use of reliable and secure deletion software, or by restoring an encrypted device to factory settings. Users shall always check their devices for SIM or SD cards (or other storage media) to determine if they require destruction or permanent removal of CAP-owned data. Users should also remember that they may have stored data in a cloud environment and should contact their provider to ensure that stored data is deleted when no longer required for business purposes. Members must work with their unit IT Officers to ensure that disposal of data is complete.

11.4. CAP data stored on CAP-owned devices will be disposed of by NHQ IT staff or at their direction using methods such as physical destruction (if the device is not to be used again), the use of reliable and secure deletion software, or by restoring an encrypted device to factory settings. The device will be checked by NHQ IT for SIM or SD cards (or other storage media) to determine if they require destruction or permanent removal of CAP-owned data. Users must ensure that data stored in a cloud environment is deleted by service providers after it is no longer required.

11.5. All CAP supplied devices will be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the computer will be unattended. This policy also applies to personally-owned devices that contain CAP data.

11.6. Data backups are to be executed to ensure data is available and useful when needed. Members responsible for CAP-owned IT assets and/or field developed systems must perform full backups no less than once a month and incremental backups weekly to protect against possible loss of information due to fire, natural or man-made disaster, or storage device failure. Back-up electronic files should be stored in another physical location (different building) so that a single catastrophic event is not likely to damage/destroy both the primary and back-up records. Members holding CAP data on their personally-owned devices are encouraged to backup any critical data and must safeguard data, wherever it resides, in accordance with this regulation.

11.7. Directors of IT or unit IT Officers must ensure that, at a minimum, the default anti-virus protection is operational on all CAP issued computers. Free anti-virus software is available through eServices for CAP issued computers.

12. Email Policy.

12.1. Proper Use of CAP Email Systems.

12.1.1. CAP reserves the right to review, audit, intercept, access and disclose all CAP.gov messages created, received or sent over the system for any purpose. The content of electronic mail properly obtained for legitimate business purposes may be disclosed within Civil Air Patrol without your permission. Users shall not assume electronic communications are totally private and confidential; you should transmit highly sensitive information in other ways, whenever possible using approaches such as encryption, fax machine to fax machine communications (not including electronic facsimile services), or manual means.

12.1.2. Owners of CAP group emails should ensure that distribution lists accurately reflect those with a need for the information provided to them.

12.1.3. CAP Email Systems shall not be used for:

12.1.3.1. Sending unsolicited e-mail messages, such as the sending of "junk mail" or unauthorized advertising material to individuals who did not specifically request such material (e-mail spam).

12.1.3.2. Transmission, retrieval or storage of discriminatory, derogatory, or harassing communication, or usage in any way that determined by command staff as insulting, derogatory, or offensive by other persons or harmful to morale.

12.1.3.3. Unauthorized use, or forging, of e-mail header information.

12.1.3.4. Solicitation of e-mail for any e-mail address other than the member's account, with the intent to harass or to collect replies.

12.1.3.5. Creation or forwarding "chain letters", or "pyramid" schemes of any type.

12.1.3.6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

12.1.3.7. Access to another user's email account without A) the knowledge or permission of that user - which should only occur in extreme circumstances, B) the approval of General Counsel in the case of an investigation, or C) when such access constitutes a function of the member's normal job responsibilities.

12.1.3.8. Sending any emails that may cause embarrassment, damage to reputation, or other harm to the organization. This includes using offensive or unprofessional email addresses that reflect poorly on the organization to conduct Civil Air Patrol business.

13. Reporting a Security Incident.

13.1. Types of Incidents. A security violation can come in many forms including a malicious attacker gaining access to the network, a virus or other malware infecting computers, or a stolen mobile/smart devices device containing confidential information. This policy covers all incidents that may affect the security and integrity of Civil Air Patrol's information assets. In all cases, it is the responsibility of the member to notify their IT Officer and the NHQ Deputy Director for IT as soon as a security incident is suspected.

13.2. PII Data Breach. In the case of a breach of PII data, the requirements of CAPR 1-2(I) that include notification to the General Counsel's office apply, in addition to notifications described above. Upon receiving notification, the NHQ Deputy Director for IT will provide guidance as to what containment actions need to be taken for any technical mitigation. The NHQ Deputy Director for IT will coordinate with the General Counsel's office regarding any potential legal considerations as well as the Inspector General Staff, where applicable.

13.3. In the event of a lost or stolen mobile/smart device containing CAP data it is the member's responsibility to report it immediately to the NHQ Deputy Director for IT.

13.4. In the event of a data breach, all compromised data shall be considered as confidential until otherwise determined by post event investigation.

14. Enforcement.

14.1. Civil Air Patrol leadership at all command levels will enforce this policy. Violation of this guidance has potential to introduce risk to Civil Air Patrol's information systems.

14.2. Resolution of Policy Violations. 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 involve National Headquarters and/or appropriate unit, group, wing or region commanders in:

14.2.1. resolving the matter informally; and/or

14.2.2. initiating disciplinary proceedings; and/or

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

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

14.2.5. 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, or local law enforcement authorities) for a prohibited CAP internet operation conducted on equipment or a domain outside of CAP's immediate control.

JOSEPH R. VAZQUEZ
Major General, CAP
Commander

Attachment 1 - Compliance Elements

Check list and Tab	#	Compliance Question	How to Verify Compliance	Discrepancy Write-up	How to Clear Discrepancy
CI	01	Has the wing published any supplements or operating instructions, or requested and been granted any waivers to CAPR 120-1? a). Is the wing operating under any supplements or operations instructions to CAPR 120-1, and, if so, were they approved IAW this regulation prior to implementation b). Is the wing operating under any waiver to CAPR 120-1 and, if so, were they approved IAW this regulation prior to implementation?	Compare wing's published supplements/OIs or waivers with those documents posted on the CAP publication website	a). (Discrepancy): [xx] (D9 Question 1) Wing failed to obtain approval IAW CAPR 120-1 para 3 for requested waiver prior to implementation IAW CAPR 120-1 para 3. b). (Discrepancy): [xx] Wing failed to obtain approval IAW CAPR 120-1 para 3 for requested waiver prior to implementation IAW CAPR 120-1 para 3.	a). Attach a copy of the approved supplement/OI or documentation confirming rescission to the Discrepancy Tracking System (DTS). b). Attach a copy of the approved waiver or documentation confirming rescission to the discrepancy in the Discrepancy Tracking System (DTS).
	02	Does the Wing have an assigned Director of IT or IT Officer responsible for maintenance, upkeep and compliance with regard to use of all CAP IT assets within their respective units IAW CAPR 120-1 para 2.2.5?	Review duty assignments for the wing within eServices to identify whether the Wing has an assigned Director of IT or IT Officer	(Discrepancy):[xx] (D9 Question 2) Wing does not have an assigned Director of IT/IT Officer IAW CAPR 120-1 para 2.2.5.	Provide screen shot of updated duty assignments showing assignment of Director of IT or IT Officer to the Discrepancy Tracking System (DTS).

Check list and Tab	#	Compliance Question	How to Verify Compliance	Discrepancy Write-up	How to Clear Discrepancy
	03	Are all wing CAP Internet Operations records current IAW CAPR 120-1 para 5.2.2?	Review the Internet Operations page on eServices to determine if mod dates for Wing websites are within the current fiscal year.	(Discrepancy): [xx] (D9 Question 3) Wing failed to comply with annual Internet Operations review requirements IAW CAPR 120-1 para 5.2.2.	Attach a print screen of updated record showing current review/in compliance mod date(s) to the Discrepancy Tracking System (DTS).
	04	Are locally developed web pages dealing with confidential information clearly marked with the warning required by CAPR 120-1 para 9.2.5?	Review representational sample of unit web pages noting whether warning is present when the page is displaying confidential information.	(Discrepancy):[xx] (D9 Question 4) Wing has not properly provided warning requirement on web pages that present confidential information IAW CAPR 120-1 para 9.2.5.	Attach a print screen of the web site containing the required warning, being sure to obscure the confidential information, to the Discrepancy Tracking System (DTS).
	05	Are backups of electronic files made IAW CAPR 120-1 para 11.6?	Review unit's backup schedule documentation to ensure backups are being completed IAW CAPR 120-1 para 11.6	a). Discrepancy):[xx] (D9 Question 5) Wing does not perform full backups at least monthly and incremental backups weekly IAW CAPR 120-1 para 11.6. b). (Discrepancy):[xx] (D9 Question 5) Wing does not store back-up files in another physical location IAW CAPR 120-1 para 11.6.	a). Attach a current backup schedule document that shows compliance to the Discrepancy Tracking System (DTS). b). Attach a current backup schedule/location document to show compliance to the Discrepancy Tracking System (DTS).
	06	Are the default anti-virus protections enabled on all CAP issued computers IAW CAPR 120-1 para 11.7?	Review a representative sample of CAP issued laptops for anti-virus software. This can found by navigating to the right hand corner of the task bar, locating the anti-virus software icon and opening application to identify if services are active.	(Discrepancy): (D9 Question 6) Wing failed to ensure anti-virus is enabled on CAP-issued laptops IAW CAPR 120-1 para 11.7.	Attach a print screen of updated record showing the computer is protected to the Discrepancy Tracking System (DTS).