FLORIDA WING SUPPLEMENT 1

CAP REGULATION 120-1

4 March 2022

APPROVED/K. CONYERS/CAP/IT

Information Technology

INFORMATION TECHNOLOGY SECURITY

CAP Regulation 120-1, dated 01 October 2017, is supplemented as follows:

2.2.7 Added. Group and Unit Commanders shall appoint a designee to maintain the unit website and calendar. The designee should be an ITO or PAO alongside a cadet counterpart. The Unit Commander will assume this responsibility if no one is appointed.

2.28 Added. Group ITOs will assist in creating and maintaining cloud system accounts for Group and Subordinate units

4.3. Added. This also applies to FLWG domains and programs.

7.5. Added. To ensure that access can be made to a corporate-owned computer that has lost access to the FLWG domain, a local administrator account will be made on each corporate-owned computer. This admin account will only be used under the supervision of an ITO or FLWG/IT for technical purposes. Members will use their credentials to log in to CAP systems. Members that need administrative privileges will contact their ITO or FLWG/IT for assistance.

10.1.1.4. Added. All Windows 10 or newer computers issued by CAP will have encryption and recovery options set by FLWG/IT. Older computers will be assessed on a case-by-case basis. Computers will be setup by IT prior to issue to a member or unit, or within sixty (60) days of issue if necessary.

10.2.2. Added. Personal mobile devices used by members to connect to FLWG resources directly are required to meet FLWG mobile device system security configuration requirements. Members may obtain the FLWG mobile device system security configuration requirements from FLWG/IT.

12.1.1.1. Added. This also applies to FLWG domains and resources (flwg.cap.gov and flwgcap.us).

12.1.4. Added. Any official communications to members, parents, or mission partners involving Civil Air Patrol business will utilize the wing-provided email system or document platform or another CAP-owned platform. Emails or documents containing any operational data, personal information, or any other restricted information will not be sent outside of CAP-owned platforms. An exception will be made for communicating with cadet parents and mission partners as needed.

12.1.4.1. Added. Members shall not set up their FLWG accounts to automatically forward FLWG email correspondence to a non-CAP domain email account. Any automatic forwarding from FLWG domain to a personal account will be removed.

12.2. Added. Parents or legal guardians of FLWG cadets may request a limited access account to have oversight of their cadet's internet activities on FLWG domain resources. Requests for such account will be submitted to FLWG/IT utilizing a FLWG Form 120G. Such accounts should be requested only after all other means of oversight are exhausted.

13.5. Added. A member preparing a Report of Survey involving CAP IT systems, shall contact FLWG Logistics for disposition. Any member knowing of any loss, theft, damage, destruction, regulation violation or violation of law involving any CAP IT systems shall advise FLWG/LG (A/4) and route it to FLWG/IT.

14.3. Added. Violations of this supplement will be enforced in accordance with CAPR 120-1, para. 14.

15. Support

15.1 Added. Helpdesk support will be provided to any member needing assistance with any MS O365 applications. A link is provided on the FLWG website https://flwg.cap.gov/

15.2 Added. FLWG/IT will support all current MS O365 applications. This will include the creation of distribution lists for wing approved activities and groups. Please see Attachment 2 for cloud group standards.

Luis E. Negron, Colonel, CAP
Commander

Attachment 1
COMPLIANCE ELEMENTS

Checklist and Tab	#	Compliance Question	How to Verify Compliance	Discrepancy Write-up	How to Clear Discrepancy
IT	01	Are all known unacceptable use incidents reported utilizing the FLWG Form 120I?	Unit will provide copies of submitted forms, or FLWG/IT will provide access to report logs for review.	(A-Discrepancy): [xx] (Question 1) Unit failed to complete a FLWG Form 120I after discovering unacceptable use IAW FLWG Supplement 1 to CAPR 120-1, para. 13.6.	Attach a copy of the completed form to the discrepancy in the Discrepancy Tracking System (DTS). FLWG/IT will confirm completion if online method is used.
IT	02	Do all Windows 10 or newer corporate-owned computers have data encryption?	Onsite inspection of computers.	(A-Discrepancy): [xx] (Question 1) Unit failed to have data encryption turned on IAW FLWG Supplement 1 to CAPR 120-1 para. 10.1.1.4.	Attach a screenshot showing drive encryption has been enabled in the Discrepancy Tracking System (DTS).