



UNITED STATES MARINE CORPS
1ST MARINE AIRCRAFT WING
UNIT 37101
FPO AP 96603-7101

IN REPLY REFER TO
1000
10
28 MAR 2002

COMMANDING GENERAL'S POLICY LETTER 5-02

From: Commanding General, 1st Marine Aircraft Wing
To: Distribution List

Subj: 1ST MAW COMPUTER NETWORK PASSWORD POLICY

1. Purpose. To promulgate 1st Marine Aircraft Wing policy on network passwords.
2. Cancellation. Commanding General's Policy Letter 1-99.
3. Background. Unauthorized users gain access to computer systems through a variety of methods. One of the most popular methods is to obtain a copy of the system's password file and run various programs on the file to decipher easily guessed passwords. After deciphering a legitimate user's password, the intruder, or hacker, can then easily gain access to the computer system and the information it contains. Establishing a strong password may go far in protecting the 1st MAW's information resources.
4. Policy. Users shall generate their own passwords and not share them. Passwords shall be a minimum of 8 characters; containing a minimum of one uppercase alphabetic character, one lowercase alphabetic character, one numeric character and one non-alphanumeric character. Easily guessed passwords shall be avoided as well as words found in any dictionary (English or Foreign). Users shall not use family members or pet's names, dates of personal importance, and wording that is written down around the work area. Users will not write down their password. The following criteria shall apply to all users. The following example is provided:
 - Use a phrase that is easy to remember. For example, try "eight character passwords are hard to crack!", which could turn into "8cPrH2C!"
5. Security. To technically enhance password protection, system administrators shall ensure the following minimums are set:

Subj: 1ST MAW COMPUTER NETWORK PASSWORD POLICY

(a) Every account shall have a password in accordance with paragraph 4.

(b) Programs shall be checked for default settings which save passwords and may permit unauthorized access. These settings shall be disabled.

(c) "Default" accounts for visitors are not created. When assigning accounts to visitors or guests, create unique accounts which expire at the projected date of the visitor's departure.

(d) Access and use of the Administrator and Ex-Administrator's accounts is limited. Instead of logging on to either of these accounts, ensure that each System Administrator has the appropriate permissions to fulfill their duties.

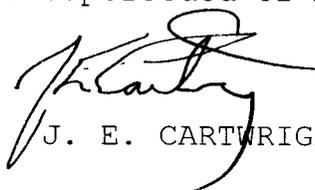
(e) Review and verify that proper permissions and access is granted for all file systems and shares.

(f) Force passwords to expire every 90 days and require that the last 10 passwords be unique.

(g) Accounts which have been dormant for more than 30 days are disabled. Delete all disabled accounts after 45 additional days.

(h) The anonymous File Transfer Protocol area is configured correctly to allow only authenticated users access to the system.

6. Applicability. This policy applies to all 1st MAW Commands and will remain in effect until superseded or modified by CG, 1st MAW.


J. E. CARTWRIGHT

Distribution: List 1, 2, 3