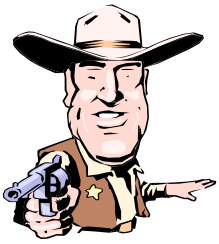
5.5 AUTHENTICATE USERS: STRICTLY ENFORCE PASSWORD SECURITY

Like a secret word or phrase used by the members of a private club, the computer password identifies the user as having the privilege to enter. A computer password consists of a word or a string of characters that is recognized by the computer to allow a user access to protected storage, files, and input and output devices. It should be a unique set of digits and/or characters to verify a user's authentication in communication with the computer. User authentication is verified with the password at the time of user login to ensure that only authorized individuals gain access to the network. In general, user passwords should always be required to gain access to the network.

To ensure effective password security, these procedures should be followed without exception:



A. Force users to change their passwords at regular intervals. Set an expiration date or number of days (e.g., 40 days) after which the user password expires (with a grace period set as the number of additional logins allowed until the password is disabled).

B. Create a different "unique" password each time. Require users to come up with a different password that is not similar to one recently used (within last eight changes).

C. Choose a "nonguessable" password. Require network users to have a password with at least six characters (eight is even better) made up of mixed-case letters, numbers, and special characters. Discourage users from using their name, birthday, pet's name, friend's name, or a password easily guessed.

D. Keep passwords confidential. Instruct employees not to write down or reveal their password to anyone. If a user forgets his or her password, the network administrator can help them establish another. Password security is ineffective if passwords are not kept confidential.

E. Do not share passwords with other employees, temps, or guests. Instruct employees not to lend passwords to others. Each user has access to different files based on the rights assigned to them by the network administrator. These access rights may not be appropriate for others.

F. Use the screen saver password protection feature (if available). If this feature is used, a workstation display will remain in screen-saver animated mode until the user returns and types in the password.

G. Log off workstations when they are left unattended or not in use. If you do not have a screen saver password feature, log off if you leave your PC unattended or are no longer using it. Whether intentionally or by accident, others may delete, damage, or copy important network files from unattended workstations.

H. User accounts and passwords of terminated employees, guests, and temps should be disabled immediately. Terminated employees' access rights, passwords, and user IDs should be revoked immediately upon notice of discharge.