Guidelines on Password and Accounts

Do:

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every three months.

- All user-level passwords (e.g., email, web, desktop computer, etc.) allocated must be changed at the first logon.

- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

- Passwords must not be inserted into email messages or other forms of electronic communication.

- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

- Always practice “clear screen” policy for information processing facilities (e.g., computer/terminals are logged out and desks are cleared of sensitive info.

Don’t:

- Reveal a password over the phone to ANYONE
- Reveal a password in an email message
- Reveal a password to the boss
- Talk about a password in front of others
- Hint at the format of a password (e.g., "my family name")
- Reveal a password on questionnaires or security forms
- Share a password with family members
- Reveal a password to co-workers while on vacation
- Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).
- Write passwords down and store them anywhere in your office.
- Store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.