General Guidelines for Password construction and protection.

a. Passwords are used for various purposes. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

b. Weak passwords have the following characteristics:
   - The password contains less than eight characters
   - The password is a word found in a dictionary (English or foreign)
   - The password is a common usage word such as:
   - Names of family, pets, friends, co-workers, fantasy characters, etc.
   - Computer terms and names, commands, sites, companies, hardware, software.
   - Birthdays and other personal information such as addresses and phone numbers.
   - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
   - Any of the above spelled backwards.
   - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

c. Strong passwords have the following characteristics:
   - Contains a minimum of 8 characters
   - Contain three of the following four character categories
   - English upper case characters (A-Z)
   - English lower case characters (a-z)
   - Base 10 digits (0-9)
   - Non-alphanumeric characters (eg !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
   - Are not a word in any language, slang, dialect, jargon, etc.
   - Are not based on personal information, names of family, etc.
   - Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered.

Password Protection Standards

a. Do not use the same password for Southwest accounts as for other non-Southwest access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various Southwest access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for a Domain account and a UNIX account.

b. Do not share Southwest passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Southwest information.

c. If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

d. Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

e. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

f. Change passwords according to frequency noted in Policy 4:02:20:00/37.

g. If an account or password is suspected to have been compromised, report the incident to Office of Information Services and change all passwords.

h. Password cracking or guessing may be performed on a periodic or random basis by Office of Information Technology or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Passphrases

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

a. A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

b. One way to do this is create a passphrase based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the passphrase could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

c. All of the rules above that apply to passwords apply to passphrases.