

- ! Contain both upper and lower case characters (e.g., a-z, A-Z)
- ! Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-
=\`{}[]:;'<>?,./)
- ! Are at least eight alphanumeric characters long.
- ! 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. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for <Company Name> accounts as for other non-<Company Name> access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various <Company Name> 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 an NT account and a UNIX account.

Do not share <Company Name> passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential <Company Name> information.

Here is a list of "don't's":

- ! Don't reveal a password over the phone to ANYONE
- ! Don't reveal a password in an email message
- ! Don't reveal a password to the boss
- ! Don't talk about a password in front of others
- ! Don't hint at the format of a password (e.g., "my family name")
- ! Don't reveal a password on questionnaires or security forms
- ! Don't share a password with family members
- ! Don't reveal a password to co-workers while on vacation

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

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

Again, 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.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

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

C. 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.
- ! should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the <Company Name> Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

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 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:

"The*?#>*@TrafficOnThe101Was*&!#ThisMorning"

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

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms

Application Administration Account
(e.g., Oracle database administrator, ISSU administrator).

Definitions

Any account that is for the administration of an application

7.0 Revision History