Password Policy
Best Practices

1.0 Overview

Passwords are an important aspect of information security, and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of RAMSRENT's™ entire corporate network. As such, all RAMSRENT™ employees (including contractors and vendors with access to RAMSRENT™ systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any RAMSRENT™ facility, has access to the RAMSRENT™ network, or stores any non-public RAMSRENT™ information.

4.1 Policy

4.2 General

- 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 three months.

- User accounts that have system-level privileges granted through group memberships or programs 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.

- All user-level and system-level passwords must conform to the guidelines described below.

4.3 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at RAMSRENT™. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e. dynamic passwords which are only used once) everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than fifteen 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.
    - The words "RAMSRENT™", "sanjose", "samara" or any derivation.
    - 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)

Strong passwords have the following characteristics:

- 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 fifteen alphanumeric characters long and is a pass phrase (Ohmy1stubbedmyt0e).
- Is 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 all RAMSRENT™ accounts as for other non-RAMSRENT™ access. Where possible, don't use the same password for various RAMSRENT™ access needs. Do not share RAMSRENT™ passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

Here is a list of "dont'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

Do not use the "Remember Password" feature of applications

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 three months (except system-level passwords which must be changed quarterly). The recommended change interval is every three months.

If an account or password is suspected to have been compromised, report the incident to management or the Head of Information Security and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis.

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.

D. Use of Passwords and Pass phrases for Remote Access Users

Access to the RAMSRENT™ Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase.

E. Pass phrases

Pass phrases 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 pass phrase to "unlock" the private key, the user cannot gain access.

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

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

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

All of the rules above that apply to passwords apply to pass phrases.

5.0 Enforcement

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