

RACC Password Policy

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of RACC's resources. All users, including contractors and vendors with access to RACC systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

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

Scope

The scope of this policy includes all members of the college 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 RACC facility, has access to the RACC network, or stores any non-public RACC information.

Policy

General

- All user accounts must be associated to an individual college member who is responsible for the security of that account.
- All user-level and system-level passwords must conform to the guidelines described below.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
- 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.
- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.

Guidelines

Password Protection Standards

- Passwords should never be written down or stored on-line without encryption.
- Do not share RACC passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential RACC information.
- Always use different passwords for RACC accounts from other non-RACC access (e.g., personal ISP account, option trading, benefits, etc.).
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to Information Technology Services.

If an account or password compromise is suspected, report the incident to Information Technology Services.

General Password Construction Guidelines

Passwords should be as strong as possible whilst still remaining memorable. All users at RACC should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
 - Lower case characters
 - Upper case characters
 - Numbers
 - Punctuation
 - “Special” characters (e.g. @#\$%^&*()_+|~-=\`{}[]:;'<>/ etc)
- Contain at least fifteen alphanumeric characters.

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)

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!)

Application Standards

Application must ensure their programs contain the following security precautions.

Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall 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.
- Shall support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval wherever possible.

Enforcement

Any college member found to have violated this policy may be subject to disciplinary action. Password cracking or guessing may be performed on a periodic or random basis by Information Technology Services or its delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

Revision History

• Version	Author	Date
1.0	Alan Benson	October 2011