Password Policy

Password Security

Password Security is an integral aspect of information security. As passwords are the first layer of protection for user accounts, a poorly chosen (weak) password may result in a compromise of personal user information and possibly confidential Regent University information. As such, all Regent University faculty, staff, and students (including visitors, contractors, and vendors with access to Regent University systems) are responsible for taking appropriate measures, as outlined below, to select and secure passwords.

Application

The purpose of this policy is to establish a standard for creation of strong passwords and protection of those passwords. This policy applies to all persons who have or are responsible for an account (or any form of access that supports or requires a password) on any system managed by Regent University, has access to the Regent University network, or stores any non-public Regent University information. This also applies to passwords for non-user accounts such as, but not limited to: service accounts, test accounts, temporary accounts and vendor accounts.

Password Privacy Statement

Notwithstanding utilization of a secret password, users of the University's computer system assets maintain no personal privacy rights with respect to content created, stored, received or sent from the University's information systems. In accordance with the Regent University Acceptable Use Policy, Regent University, or its delegates, reserves the right to intercept, monitor, or record all information stored on its information systems and inspect activity to diagnose problems or identify security threats and/or violations.

Password Selection Guidelines

Passwords are used for various purposes within Regent University. For this reason, all users of Regent University managed assets should understand how to select strong passwords.

A strong password has the following characteristics:

- Contains no less than fourteen (14) characters
- Contains at least one upper case alpha character (A-Z)
- Contains at least one lower case alpha character (a-z)
- Contains at least one numeric character (0-9)
- Contains at least one allowed non-alphanumeric character !*-._+:?[\]^~
- Is not based on personal information, names of family, etc.
- Best practice is to use a "pass phrase" of something that you can remember, such as a song lyric with mixed case and non-alphanumeric characters and numbers separating the words in the phrase
- Password length, character for character, is more important than password complexity

A poor, weak password has the following characteristics:

- Contains less than 12 characters
- Is a common usage word such as:
    - Names of family, pets, friends, co-workers, teams, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software
    - The words "RegentUniversity", "vabeach", "cbn" or any derivation
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or keyboard patterns like aaabbb, qwerty, zxcvbn, 123321, etc.
    - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Additional weak or poor quality password information can be found here:
https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Password Secrecy Guidelines
The following suggestions provide a guideline for protecting password secrecy.

- Never share passwords with anyone, including instructors, assistants, technology service staff, or supervisors, either verbally, via email, fax, photocopy, or any other means of communication. IT may request that you change your password but will NEVER as that you disclose it.
- Do not re-use passwords used on any external accounts (personal email, social media, shopping sites, etc.)
- Do not write down passwords on paper and store them in insecure places
- Use a trusted password management application such as Bitwarden or 1Password
- Change passwords immediately if compromise is suspected

Password Aging and Expiration
In accordance with this policy, all users must change any Regent University managed password in their control, at a minimum, every 365 days. Passwords exceeding this limitation are subject to enforcement as defined in the 'Password Policy Enforcement' paragraph of this policy.

Password Policy Enforcement
Regent University, or its representatives, reserves the right to utilize password auditing tools on any University managed asset. Users found to employ weak or aging passwords will be notified and required to change their password to one in compliance with this policy. Password changes may also be prompted as a result of a suspected compromise of any account using a Regent username or email (internal or external.) Users may report any violation of this policy to the Regent University Help Desk at (757) 352-4076 or abuse@regent.edu. Violating any portion of this policy may result in suspension of Regent University computer access or other action as directed by University policy or, where applicable, by law.

Further References
SANS Institute Password Best Practices: https://www.sans.org/blog/everything-you-need-to-know-about-passwords-for-your-organization/
CISA Password Guidelines: https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords
NIST Technical publication 800-63B: https://pages.nist.gov/800-63-3/sp800-63b.html