WELLESLEY

Wellesley College
Password Guidelines

Overview

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

Purpose

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

General Password Construction Requirements

- Has at least 8 characters
- Has at least three of the four character types:
  - Uppercase letter
  - Lowercase letter
  - Number (0 – 9)
  - Special character. E.g. ? $ # ( ) !
- Does not contain words in any language, slang, dialect, jargon, etc., even if they are separated by numbers or special character (e.g. be87gin)
- Does not contain repeated characters or a sequence of keyboard letters. E.g. qwerty, 12345, or yyy99
- Does not contain any part of your name, username, birthday, or social security or those of your friends and family. E.g. Jill1030

Password Management Guidelines

- Passwords must be changed at least annually.
- Passwords should not be shared with others. In cases where password sharing is unavoidable, restricted accounts should be established to protect information resources.
- Passwords, if they need to be written down or stored on-line, must be stored in a secure place separate from the application or system that is being protected by the password. (i.e., no sticky-notes posted on the computer)
- Do not respond to email or phone requests to reveal username and password information.

- Do not use the “remember password” feature of applications unless the system or application has the means to encrypt the remembered password.
- Do not use Wellesley passwords for non-Wellesley sites. E.g. Gmail or Facebook
- Set browser defaults to clear password information each time the user exits the browser.
- Do not choose reset questions that may be easy for others to guess. E.g., Q: Name your favorite team: A: Red Sox
- If an account or password is suspected to have been compromised, report the incident to the Information Security Officer immediately and change all passwords.
- Password cracking or guessing may be performed on a periodic or random basis by the Information Security Officer or his delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.