PASSWORD POLICY

Responsible Office**: Information Technology**
Date Created 12/14/2018
Next Update: 12/14/2019

Webster University
Password Policy

POLICY STATEMENT

All constituents at Webster University must access a variety of resources, including computers, hardware devices, data storage systems, and other accounts. Passwords are a key part of Webster University's strategy to make sure only authorized people access those resources and data. Passwords help ensure the security and confidentiality of the data stored or accessed on our systems and devices, however their effectiveness as a security measure depends on individual password strength and our community's adherence to industry standard practices.

RELATED POLICIES

Acceptable Use Policy

POLICY PURPOSE

Passwords are the primary form of user authentication used to grant access to Webster University's information resources. To ensure that passwords provide as much security as possible they must be carefully created and used. Without strict usage guidelines the potential exists that passwords will be created that are easy to break thus allowing easier illicit access to Webster's information resources. This policy covers all users who are responsible for one or more accounts or have access to any resources that require a password.

DEFINITIONS

Password - A secret series of characters that enables a user to access a file, computer, or program.

Passphrases - A passphrase is a longer version of a password and more meaningful to the user.

Authentication --- the process of confirming the correctness of the account holder's identity. User authentication focuses on verifying a person's identity based on the reliability of a credential offered, typically a password. Verification answers the question, "How sure am I that you are who you say you are?"

Information Security --- Information security refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

Information technology resources --- Includes voice, video, data and network facilities and services.

Network (computer network) – A network is a collection of computers and devices connected by communications channels that facilitates communications among users.

POLICY

General

Password Construction Guidelines

- All passwords should be complex and difficult for unauthorized entities to guess. Users should choose passwords that are at least twelve (12) characters long and contain the following: upper---case letters, lower---case letters, numbers, and at least one special character (Only the following special characters are permissible: **~!@#$---+=|(){}[]:;,.?**).

- In addition to these requirements, users must avoid basic combinations that are easy to break. For instance, choices like "password," "password1", and "Pa$$w0rd" are equally ill-advised from a security perspective. Users are discouraged from using any similarities with their user name in the password

- A password should be unique, with meaning only to the person who chooses it. One recommended method to choosing a strong password that is still easy to remember: Create a **PASSPHRASE** – identify a phrase that is easy to remember, and then replace some of the letters with numbers, special characters, or vary capitalization. For example, the phrase "I do not like it" can become "**!don0tlikeit"**.

- Users must choose unique passwords for their University accounts, and should not use a password that they are already using for a personal account.

This means that the password you use to access Webster University services should not be one that you use for any non-Webster account.

- If the security of a password is in doubt; for example, if it appears that an unauthorized person has logged in to the account, the password must be changed immediately.

- Default passwords – such as those created for new users when they're initially setup, must be changed as quickly as possible.

Protecting Passwords

- Users may never share their passwords with anyone else in the University, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique account and password.

- Users may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system. If in doubt, check with your supervisor.

- Users must refrain from writing passwords down and keeping them at their workstations.

- Passwords should never be transmitted electronically over the unprotected Internet, such as via email.

Password Lifecycle

- Passwords will have a maximum age of 180 days. Users will be required to change their passwords 180 days from the last time it was changed. For critical services (i.e. CX), the maximum age is 60 days.

- Passwords may be reused every thirteenth password. As such, a completely new password is required for the first twelve (12) resets; thereafter, the first password can be reused, and so on.

- "Completely new" is defined as having at least fifty percent (50%) of the characters different from the previous password.

Non-Compliance

Any violation of this policy may result in disciplinary action, up to and including termination of employment. The University reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.