Responsible Office: Information Technology
Date Created: 7/20/2016
Last Updated: 9/6/2016

Webster University
Password Policy

POLICY STATEMENT

Students, faculty and staff at Webster University must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of IT's strategy to make sure only authorized people can access those resources and data.

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, thereby compromising the security of those resources. This policy covers all users who are responsible for one or more accounts or have access to any specified 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, therefore more secure.

Authentication - the process of confirming the correctness of the claimed 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** – a phrase is taken that is easy to remember, and then some of the letters are replaced with numbers or special characters, or the capitalization is varied. For example, the phrase "I do not like it" can become "**!don0tlikeit"**. This is extremely secure and hard to hack, but easy to remember.

- 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 start or those that protect new systems when they're initially set up – 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 password.

  NOTE: When troubleshooting a problem with certain technology services (Connections and WorldClassRoom), the Webster IT Service Desk may ask you for your password, during your inquiry over the phone, in order to try to replicate your issue. You always have the option say no, but the Service Desk may not be able to assist you if you refuse. If you do give the Service Desk your password, you always have the option of changing it immediately after. No passwords are ever saved, but are immediately shredded.

- 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 should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All users will receive training on how to recognize these attacks.

- Users must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

- Users may not use password managers or other tools to help store and remember passwords without IT's permission.

- Passwords should never be transmitted electronically over the unprotected Internet, such as via email. (**Please note: The initial password will be sent via personal email to users going forward, but users will be required to change the initial password immediately).

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.
- Passwords may be reused every thirteenth password. As such, a completely new password is required for the first twelve (12) expires; 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.
- Password accounts will be locked out after five (5) unsuccessful attempts. The account will remain locked until a successful unlock has been processed through the self-service password reset and unlock tool, or via contact to the Service Desk.

RELATED PROCEDURES:

RBAC (Role Based Access Control) Procedures for O365 and Directory Services (linked)

Role Hierarchy and Transition Procedures for O365 and Directory Services (linked)