FITCHBURG STATE UNIVERSITY

52 - Passwords

Issued 8/15/2022

Version 1.0

Purpose

Fitchburg State University (hereafter referred to as “Fitchburg State”) utilizes passwords to provide secure access to a number of important electronic systems and applications. This policy establishes a standard for the creation, maintenance and usage of passwords within Fitchburg State systems.

Scope

This policy applies to anyone receiving an account on any Fitchburg State system.

Policy

Your “Falcon Key” account is a user ID and password that serves as the primary digital identity at Fitchburg State. It works in tandem with Fitchburg State’s Active Directory and LDAP (Lightweight Directory Access Protocol) to provide the foundation of authentication (who you are) and authorization (what you can do).

Fitchburg State requires that the guidelines below are followed when accessing secure systems at the University. This applies to all personnel, students, business partners, contractors and consultants utilizing Fitchburg State electronic systems, regardless of their actual physical location:

* Whenever possible, systems will rely on the University’s Active Directory system to integrate username/password information. Two-factor systems shall be used whenever possible to further protect against attackers exploiting credentials to gain access to data and systems.

* Each user is responsible for maintaining the confidentiality of passwords that are used to gain access to University systems and services.

* Passwords should not be shared with anyone, including assistants. All passwords are to be treated as sensitive, confidential information. It is permissible to share your password with Information Technology support personnel for troubleshooting purposes only and you should change your password immediately after the work is performed.

* Passwords used to gain access to non-University systems or services should not be used as passwords to gain access to University systems or services.

* If a password is compromised or believed to be compromised, users will inform the Help Desk and, if possible, changed immediately.

* Passwords should not be written down or stored electronically without encryption.

* Users should never attempt discovery of a system or another user’s passwords.

Password Composition and Restrictions
The following conventions shall be used whenever creating a password. The password shall:

* Contain at least 8 characters but not more than 15.
* Not be a word found in the dictionary.
* Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
* Contain characters from three of the following four categories:
* English uppercase characters (A through Z)
* English lowercase characters (a through z)
* Base 10 digits (0 through 9)
* Non-alphabetic characters (for example, !, $, #, %)
* Be changed at least every 90 days, have five grace logins and will be expired thereafter.

Invalid username/password login attempts will be limited to five successive incorrect logins and then the account will be locked for 5 minutes from further attempts.

The six prior passwords will not be available for reuse.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including loss of access rights and/or termination of employment under adherence to their respective collective bargaining agreement. Students found to have violated this policy may have their access removed and may have additional actions taken as directed by the Student Code of Conduct.

Security Level Public