FITCHBURG STATE UNIVERSITY

Password Policy

Version 2.0	**Last Updated:** 5/22/2024
Security Level: Public	**Issued:** 8/15/2022

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. This includes all personnel, students, business partners, contractors and consultants regardless of there actual physical location.

Policy

Your Fitchburg State credentials, also known as a “Falcon Key” account, are a user ID and password that serve as your primary digital identity at Fitchburg State. The account works with Fitchburg State’s Identity and Access Management services 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.

- Systems will rely on the University’s Identity and Access Management system whenever possible to integrate username/password information.
- Multi-factor authentication (MFA) shall be applied whenever possible to further protect against attackers exploiting credentials to access data and systems.
- Each user is responsible for maintaining the confidentiality of passwords used to access 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 the Technology Department’s support personnel for troubleshooting purposes only, and you should change your password immediately after the work is completed.

- 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 Technology Help Desk and, if possible, change it immediately.
- Passwords should not be written down or stored electronically without encryption.
- Users should never attempt to discover a system or another user's passwords.
- Invalid username/password login attempts will be limited to ten successive incorrect logins and then the account will be locked for 30 minutes from further attempts.

Password Composition and Restrictions

The following conventions shall be used whenever creating a password/passphrase.

Standard Users:

A standard user is someone who does not have access to make administrative or privileged changes in the domain.

1. At least 12 characters
2. Be changed every 360 Days
3. Not be comprised of just a single word found in the dictionary
4. Not be a previously compromised password or passphrase
5. Not be one of the six previous passwords used
6. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.

Privileged and Service Accounts:

1. Privileged accounts must be at least 16 characters,
2. Service accounts must be 20 characters or change automatically
3. Privileged accounts must be changed every 90 days.
4. Contains characters from at least three of the following categories:
    a. Uppercase characters (A through Z)
    b. Lowercase characters (a through z)
    c. Base 10 digits (0 through 9)
    d. Special characters (for example, &, $, #, %)
5. Not comprised of just a single word found in the dictionary
6. Not be a previously compromised password or passphrase
7. Not be one of the six previous passwords used
8. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.

Roles

Campus Members: Understand and adhere to this policy.

Technology Staff: Follows this policy and enforces the requirements above. Assists in educating constituents on this policy and how to create strong passwords.

CISO/ISO: Ensure compliance with this policy, maintain and implement it, and continue to provide community training regarding it.

References

CISV8 - Control 5, Account Management

PCIv4 - Requirements 8.1,8.4

MA 201 CMR 17.00 Section 17.04

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.

Revision History

Date of Change	Revision	Responsible	Summary of Change
8/15/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Creation of Policy, Start of Revision Tracking, Formatting of Document
4/17/2024	1.1	Eric Boughton, CISO	Adjusted requirements, References, and formatting.
5/22/2024	2.0	Eric Boughton, CISO Stefan Dodd, CIO	Adjusting Requirements to 12 characters and defining standard and privileged accounts