Password and Multi-Factor Authentication (MFA) Policy

All users are required to establish a network password and enroll in Multi-Factor Authentication (MFA) before accessing institutional systems and data.

Account Activation

When a new account is created, an account activation email containing a secure registration link will be sent to the user's personal email address on file. The activation link is valid for 48 hours.

Users must complete account registration within 48 hours by:

- Creating a network password.
- Enrolling in the institution's approved MFA solution.
- Verifying their identity through the registration process.

Accounts that are not activated within the required timeframe may require assistance from Information Technology Operations to complete activation.

Password Requirements

Passwords serve as the first line of defense against unauthorized access. Users are responsible for creating and maintaining secure passwords.

Network passwords must:

- Be at least 8 characters in length.
- Contain a combination of letters, numbers, and/or special characters.
- Not contain the user's name, username, employee ID, student ID, or other easily identifiable personal information.
- Be unique and not reused from other personal or professional accounts.
- Not match any of the user's previous five passwords.

Users are encouraged to create passphrases consisting of multiple unrelated words that are easy to remember but difficult to guess.

Multi-Factor Authentication (MFA)

MFA is required for all accounts and provides an additional layer of security beyond a password.

Users must:

- Maintain at least one registered MFA method.
- Immediately update MFA methods when changing devices or phone numbers.
- Notify Information Technology Operations if access to their MFA device is lost or compromised.
- Never approve MFA prompts that they did not initiate.

Unexpected MFA prompts may indicate an attempted account compromise and should be reported immediately.

Password Security Requirements

To protect institutional information and systems, users must:

- Never share passwords with anyone, including supervisors, co-workers, student employees, contractors, family members, or friends.
- Never disclose passwords over the phone, email, text message, chat application, or online form.
- Never write passwords in unsecured locations or store them in plain text.
- Never allow another individual to use their account credentials.
- Use the google password management software when storing passwords.
- Lock or sign out of devices when leaving them unattended.

Reporting Suspected Compromise

Users who believe their password, MFA device, or account may have been compromised must immediately:

1. Change their password, if possible.
2. Notify Information Technology Operations at 518-244-4777 or via sc.sage.edu
3. Follow any additional security instructions provided by Information Technology Operations staff.

Prompt reporting helps protect institutional systems, data, and community members from unauthorized access.

Compliance

Failure to comply with this policy may result in suspension of account access and may be subject to disciplinary action in accordance with institutional policies.

Revised July 2024
Revised June 2025
Revised June 2026