Policy: SEU Password Policy

Policy Details

Revised: Nov.1, 2024

Author(s): Heather De La Cruz, Security Analyst
Joshua Rhoden, Director of Infrastructure and Security
Neal Dyer, Chief Technology Officer

Effective: Nov.1, 2024

Audience: All personnel accessing Southeastern University's information systems

Introduction:

Southeastern University (SEU) is committed to prioritizing the security and confidentiality of digital assets, information systems, and data. SEU identifies requirements for secure password practices.

Purpose:

To establish acceptable secure password practices

Scope:

This policy applies to all employees, contractors, consultants, temporary workers, students, and other personnel accessing Southeastern University's information systems, networks, and data.

Policy:

Password Sharing

Sharing account passwords with other individuals is prohibited. This includes sharing passwords with colleagues, supervisors, IT, or other staff and faculty. Personnel may not provide their password to anyone and are prohibited from requesting account passwords.

Breach

SEU reserves the right to disable, suspend, or reset passwords on accounts that may have been, or suspected of being breached without prior notice.

Password Complexity

Best practices include passphrases that can easily be remembered including alphanumeric and special characters.

Password History

Personnel are prohibited from reusing the last eight passwords to prevent the reuse of previously compromised passwords.

Password Storage

Passwords may not be written in physical or digital format in plain text. Examples of prohibited practices include writing a password on a sticky note, under a keyboard, in drawers or in plain text documents.

Password Recovery

Users must follow the organization's established procedures for password recovery. These procedures may include verification of the user's identity before resetting passwords.

Individual Accountability

Each user is individually responsible for the security of their login credentials, including passwords, passphrases, and any other authentication methods.

Enforcement

Users found to be in violation of this policy may also face temporary or permanent suspension of access to organizational systems and resources. If IT determines that a user's password may be compromised, they may ask the end user to reset it. If the user does not comply with the amount of time disclosed in the request, IT will lock their account and require the user to call the IT HelpDesk for user identity verification and password reset

Revision History

Date	Description of Change	Revised by	Approved by