Password Policy

Policy Statement:

This policy establishes guidelines for creating strong and secure passwords to protect the confidentiality, integrity, and availability of our organization's information assets.

Scope:

All users, including employees, students, contractors, and third-party vendors, must adhere to the following password requirements:

Password Length:

Passwords must be a minimum of 20 characters in length. Longer passwords provide increased security against brute force and dictionary attacks.

Password Complexity:

Passwords are allowed to be a phrase that can easily be remembered. Passwords containing special characters within that phrase are more secure and difficult to hack.

Password Expiry:

All passwords must be reset annually. Users will receive notifications prompting them to change their passwords before expiration.

Password History:

Users are prohibited from reusing their last eight passwords. This prevents the reuse of previously compromised passwords and enhances overall security.

Password Storage:

Passwords must not be stored in plaintext format. They should be stored securely using industry-standard encryption methods. Passwords must not be written down or stored in easily accessible locations, such as on sticky notes, under keyboards, or in desk drawers.

Password Sharing:

Users are strictly prohibited from sharing their passwords with others, including colleagues, supervisors, or IT staff. Each user is responsible for maintaining the confidentiality of their password. Refer to the Password Protection and Confidentiality Policy.

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. You may be asked for information verifying your identity, such as the last four digits of your SSN, home address, student ID #, etc…

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.

Review and Revision:

This policy will be reviewed annually and updated as necessary to reflect technological changes, security best practices, or organizational requirements. All users will be notified of any changes to the password policy and provided with appropriate training and guidance to ensure compliance.

Conclusion:

By adhering to this policy, all users play a vital role in upholding the security and integrity of Southeastern University's digital assets and information. Together, we maintain a secure and compliant environment for conducting business operations.