Northeastern ILLINOIS UNIVERSITY

University Policy

Volume I1: Information Technology	**I1.02.1 Password Management**	**Responsible Office:** University Technology Services
Chapter 02: Data Security	**Effective Date:** 01/02/07 **Last Revised:** 05/29/24	**Responsible Officer:** Information Security Officer

POLICY STATEMENT

The use of passwords enhances access control to data and information systems and reduces the likelihood of a compromised account if the password is managed appropriately. Individuals are responsible for ensuring their passwords are reasonably strong and for maintaining the confidentiality of their passwords. Computer users must never share their passwords with others.

PURPOSE OF THE POLICY

This policy outlines the requirements for password selection and maintenance. Its purpose is to reduce the overall cybersecurity risk to the university by promoting good practices for using and managing passwords to access information systems.

WHO IS AFFECTED BY THIS POLICY

All users of University Information Technology Resources (ITR)

DEFINITIONS

University NetID: is a unique identifier assigned to individuals and is used as the account/user name for access to related IT systems. A NetID is usually a combination of names and initials with exceptions when there is a pre-existing matching NetID.

Password: is a combination of alphanumeric and special characters and/or word phrases (passphrases). It is used with a NetID and multifactor authentication (if available) to provide strong access control to university information systems.

Privileged Users: individuals with elevated or administrative rights to manage IT systems or provide technical support.

IT Service Accounts: these are accounts used for automating the operation and management of IT services or to carry out machine-to-machine or non-human interactive tasks.

Password Reset Function: is the university's self-service password reset portal.

Password Management Tool: is an online tool that helps users create, save, manage, and use passwords across different websites eliminating the need to memorize passwords or write them down.

REGULATIONS

PASSWORD CRITERIA

Computer users are required to select passwords according to the following criteria:

- A password or passphrase must be at least **12 characters long**.

- Cannot contain a NetID, first name, last name, or email address.
- Must meet the following four criteria:
    - Contain at least one uppercase **and** one lowercase character.
    - Contain at least one numeric character.
    - Contain one special character such as #, $, !, - or _) @, etc. Spaces are counted as characters in passwords or passphrases.
- A password must be unique to the user along with their unique NetID. This also applies to passwords for privileged accounts.
- This policy provides the minimum requirements for IT service account passwords. More stringent controls should apply to IT service accounts where possible, such as longer password length, the password should be changed once a year, or when someone with the knowledge of the password no longer needs it.

PASSWORD USE AND MANAGEMENT

- Only the password that meets the password criteria will be accepted.
- Passwords must not be shared with **anyone** including IT Service Desk. Where passwords must be shared to support certain business processes, this must be operated in a way that does not create a risk exposure to the related system. Login attempts and sessions must be logged.
- Passwords must not be stored or transmitted in plain text or any reversible form on university IT systems. Passwords should not be displayed in plain text as they are being entered.
- University login credentials must not be used for personal user accounts e.g., personal email, social media, payment portals, personal banking, retail stores, cloud platforms, etc.
- Where an IT system requires a local password, i.e. it is not tied to the university's Same/Single Sign On authentication (SSO), users must **not** use their SSO passwords on these systems.
- System administrators must change vendor-default passwords to IT systems before the systems go into production.

PASSWORD RESET

- Users must reset the default or given password the first time they log into a system.
- Passwords for all standard user accounts will be changed every 180 days. Some IT systems may require a password change of less than 180 days for additional security controls.
- Reuse of the six (6) most recent passwords is not permitted.

Users who forget their passwords or are locked out after failed login attempts will be required to use the self-service password reset portal to re-establish their access and create a new password. The IT Service Desk can provide some support if needed.

ENFORCEMENT AND EXCEPTION

Failure to comply with the above policies may result in the denial of access to university IT systems or disciplinary action against the user per the Acceptable Use of Information Technology Resources policy. Exceptions to the policy must be approved by the Chief Information Officer.

PROCEDURES

Approved users of the University's Information Technology Systems will adhere to the procedural directives outlined within the Regulations Section of this policy.

GUIDELINES

- Create passwords (passphrases) that you can easily remember but are difficult to guess.
- If a password must be communicated, do so in private.
- Passwords should not be included in email messages.
- Use answers that can't be guessed easily for your password reset security questions. Avoid passwords with known or public information about you, such as anniversaries, pet names, child or spouse names, sports teams, or easily identifiable or common phrases or slogans.
- Avoid using password hints.
- Watch out for emails/text messages, or calls soliciting your login details. The IT Service Desk will never ask you to provide your password or answers to your password security questions.
- If available, use MFA (Multifactor Authentication), to provide additional security for your user account.
- Use password management tools that are secure and reliable.
- Do not reuse the same password on multiple systems. If your user account is compromised on one system, it may compromise your user accounts for other IT systems.
- If you suspect your password is compromised, change it immediately and report the incident to the IT Service Desk.

HISTORY

06/30/2009 – Revised; edited responsible office
12/10/2009 – Revised; reformatted document
05/29/2024 – Revised; comprehensive review
07/25/2024 – completed 30-day public comment review
07/31/2024 - enacted

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

I1.1.1 – Acceptable Use of Information Technology Resources

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	E-Mail
IT Service Desk	(773) 442-4357	IT-ServiceDesk@neiu.edu

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for a review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.