Northeastern Illinois University

NEIU POLICY

Volume I1: Information Technology	**I1.02.1** **Strong Password**	**Responsible Office:** University Technology Services
Chapter 02: Data Security	**Effective Date:** 01/02/07 **Last Revision:** 12/10/09	**Responsible Officer:** Executive Director

POLICY STATEMENT

The integrity and secrecy of an individual's password is their responsibility. Every computer user is responsible for the security, privacy and confidentiality of Northeastern Illinois University's data to which he/she has access. Each computer user is responsible for all transactions generated thru the usage of his/her account. **Computer users must never share their passwords with others.**

PURPOSE OF THE POLICY

The Strong Password document describes the University's requirements for acceptable password selection and maintenance. Its purpose is to reduce overall risk to the institution by helping computer users reasonably avoid security and privacy risks that result from weak password choices and to encourage attention to password secrecy.

WHO IS AFFECTED BY THIS POLICY

All users of University Information Technology Resources (ITR)

REGULATIONS

1. PASSWORD CRITERIA

Computer users at Northeastern Illinois University shall select passwords according to the following mandatory criteria:

- Minimum Length: A password must be 8 characters or more in length
- Can not contain your NetID, firstname, lastname or email address
- Must meet at least three of the following four criteria:
  - Must contain at least one uppercase character
  - Must contain at least one lowercase character
  - Must contain at least one numeric character
  - Must contain one special character (#, $, !, - or _)

The following criteria are strongly recommended but not mandatory:

- Can not be a common four letter word found in the dictionary
- Can not be a password that is easy to guess, such as birthday; names of a pet, child or spouse name; or use an easily identifiable phrase like 'go cubs', 'go sox', or 'go bulls'

2. PASSWORD AGING

The minimum life of a password is one day.

All users of Northeastern Illinois University computing systems will be required to change their passwords on a regular basis. The frequency of the password change will be based upon their relationship with the university and the sensitivity of the data they are accessing.

Reuse of any of the NetID's previous 6 most recent passwords will not be permitted.

When a computer user's password expires, the computer user will not be locked out, but will be required to change their password using the Interactive Password Reset function before continuing with their login.

A computer user who forgets their password will be required to use the Interactive Password Reset function to re-establish their access to the NEIUworks application and create a new password.

If a computer user enters an invalid or incorrect password four (4) times in a row, they will be locked out of the NEIUworks application and will be required to re-establish their access and reset their password by using the Interactive Password Reset function.

Inability by a computer user to re-establish their NEIUworks access via the Interactive Password Reset function will require the computer user to contact the appropriate **NEIU*works*** University System Administrator for assistance.

Refer to the following chart for frequency information.

Relationship to University	System(s) Accessed	Security Level	Frequency of Change
Student	Personal Self Service	Low	180 Days
Employee	Personal Self Service	Low	180 Days
Employee	Financial, Human Resource, and/or Payroll Self Service	Medium	90 Days
Faculty	Blackboard Administration	Medium	90 Days
Employee	Banner Full Service	High	30 Days

3. CONSEQUENCES OF NONCOMPLIANCE

- Attempts to create or change a password to one that does not meet the above parameters will result in rejection of the change of the password.
- Accounts with expired passwords will be denied access to participating systems. Computer users will be directed to the Interactive Password Reset Function.

4. UNAUTHORIZED USAGE & ENFORCEMENT

Password hacking is a science growing ever more sophisticated, so stringent rules for passwords are required. The NetID and password assigned to you are solely for your use. Refrain from sharing your password with co-workers and other individuals.

If a computer user suspects that his password has been compromised, he/she must immediately change his/her password. Report the incident to your NEIUworks System Administrator immediately.

If a supervisor or other person demands your password, refer that person to this document and contact your NEIUworks System Administrator immediately. There are not ANY exceptions to this policy.

Failure to comply with the above policies will result in the denial of access to information in the NEIUworks Information System and/or disciplinary action against the computer user per the Acceptable Use of Information Technology Resources policy.

GUIDELINES

- Try to create a password that can be easily remembered. One way to do this is to create a password based on a song title, affirmation or other phrase. For example, the phrase might be

"This May Be One Way To Remember" and the password could be "TMB1wtr", "Tmb!WTR" or some other variation. Passwords must not be written down and stored in your office area.

- Passwords should never be stored online, including PDAs or your cellular phone without encryption enabled.
- Do not share your password with co-workers, supervisors, administrative assistants or any other individuals including the help desk/technical support staff.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Do not use the same password for university related accounts as for other non-University access. i.e.; your personal email account, options trading account or e-bay account.
- Do not share a password with family members.
- Do not reveal your password on questionnaires or security forms
- Do not hint at the format of your password.
- Computer users should logoff of any NEIUworks application when the computer user leaves his/her desk for more than 30 minutes.

HISTORY

06/30/2009 – Revised; edited responsible office
12/10/2009 – Revised; reformatted document

RELATED POLICIES, DOCUMENTS, AND LINKS

I1.1.1 – Acceptable Use of Information Technology Resources

I1.3.1 – University E-Mail

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	E-Mail
University Technology Services	(773) 442-4190	ucompute@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.