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.

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.

All users of University Information Technology Resources (ITR)

1. PASSWORD CRITERIA

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

- x

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) 0 0 scn C /P <(s)-3(s)-3(w)19(or)4(d f)15(ou)13(r)4(()4(4))4((s)-

"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.

- x Passwords should never be stored online, including PDAs or your cellular phone without encryption enabled.
- x Do not share your password with co-workers, supervisors, administrative assistants or any other individuals including the help desk/technical support staff.
- x Passwords must not be inserted into email messages or other forms of electronic communication.
- x 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.
- x Do not share a password with family members.
- x Do not reveal your password on questionnaires or security forms
- x Do not hint at the format of your password.
- x 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.