TYPE: INFORMATIONAL & INSTRUCTIONAL TECHNOLOGY

POLICY TITLE: NWTC Password Policy

Purpose

The purpose of this policy is to ensure that passwords used on systems supported by Northeast Wisconsin Technical College (NWTC) are compliant with industry best practices with regards to security, to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of changing the password.

Policy

User authentication is a means to control who has access to NWTC systems. Controlling access is necessary for all systems. Access gained by ~~a~~ non-authorized entry can have impacts on confidentiality, integrity, system availability, revenue, identity theft, liability, trust, and/or harm the reputation of Northeast Wisconsin Technical College.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password could result in the compromise of the entire network. All NWTC employees, contractors, vendors, and students with access to NWTC systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The scope of this policy includes all users who have an NWTC user account, have access to NWTC systems or network, or store any NWTC information on NWTC systems or internet/cloud-based services like Google, Dropbox, and Evernote.

Password protection is a critical step in a securing NWTC data. NWTC staff and students must adhere to the following rules for protecting passwords:

- Do not use the same password for NWTC accounts as for other non-NWTC access (personal emails account, bank account, etc.).
- Do not share NWTC passwords.
- All passwords are to be treated as sensitive, confidential information.
- Passwords should never be written down.
- To keep a password secure:
    - Don’t reveal a password over the phone or in front of others
    - Don’t reveal a password in an email or instant message
    - Don’t hint at the format of a password (e.g., "my family name")
    - Don't reveal a password on questionnaires or security forms
    - Don't reveal a password to co-workers at any time, for any reason
- Do not use the "Remember Password" feature of applications.

- Do not store passwords anywhere in your office.
- Do not store passwords in a file on any computer system unless it resides in an NWTC IIT approved virtual password vault such as Keepass.
- If an account or password is suspected to have been compromised, report the incident to the NWTC Help Desk immediately and change your suspected password.

Password Standard

The following will be used at NWTC as the standard for passwords:

- Five unique passwords will need to be used before an old password can be re-used.
- Passwords must be changed every 180 days..
- The minimum password length is 8 (eight) characters.
- In addition to the password length, a password must contain at least three of the following criteria:
    - At least one uppercase letter (A-Z)
    - At least one lower case letter (a-z)
    - At least one digit (0-9)
    - At least one non-alphanumeric character (!@#$%^&*()_+|~-=\`{}[]:";'<>?./)
      (We no longer provide temporary passwords)

Initial Password Procedure

New and returning Students who perform an account creation/activation through the my.NWTC portal may set their password at this time. New Employees and Students who register through the Enrollment Services Office must access the Password Self-Service Portal to initially set their password. It is advised that NWTC students and staff also set their own security questions through the NWTC Password Registration Portal which will be used to change their password going forward.

Password Reset

It is recommended that all NWTC users including students reset their own password through the NWTC Password Self-Service Portal: https://pwd.nwtc.edu

Students can optionally call the Student Help Desk. Contact information for the Student Help Desk can be found here.

Required Password Resets

A password can be used up to 180 (one hundred and eighty) days before the user is required to change it. An email notification will be sent to the all NWTC Personnel and Students' primary email address listed in the PeopleSoft system 30, 15 and 3 days prior to the expiration of the password. The email notice will advise the user to access the Password Self-Service Portal to change their password.

Failure to change the password will result in the user being locked out of Blackboard, student email, the network, and other systems until the password is reset through the password reset portal or the NWTC Help Desk.

Revision History

Creator	**Description**	**Submission Date**	**Approval Date**
NWTC	Old Version	Apr2008	
ADesHotel	Second Draft and Suggestions	9/13/13	
Bzimmerman	Suggestions	9/18/13	
Lhartford	Updated to remove non policy items	2/21/2014	
Brian Z, Nate W and Kevin S.	Password Reset Procedure	3/6/14	
Karl Reischl & Laurie McMoran	Edits Draft 5	03/13/14	
Nate, Brian, Scott, Karl	Edits Draft 6 to include students	07/28/14	
Nate	Proposed changes listed in RED	9/28/15	