PennWest
UNIVERSITY

Policy IT011: Password Policy

Recommended for Approval by: Fawn L. Petrosky
Fawn L. Petrosky, Vice President for Finance and Administration

Approved by: R. Lorraine Bernotsky
Dr. R. Lorraine Bernotsky, Interim President

Effective Date: 07/01/2022
Amended Date: 12/12/2023; 01/31/2024

Appropriate password security is necessary to protect Pennsylvania Western University's (PennWest) academic interactions, business and research. Passwords are often the first, and sometimes the only, defense against unauthorized access or intrusion of a specific computing system. Creating and maintaining secure passwords is an important step to protect against unauthorized use of computing resources.

This policy describes the requirements necessary for creating and maintaining password security on all PennWest User Accounts.

A. Intent

The purpose of this policy is to require a standard set of rules regarding the length, complexity and expiration time period for passwords and storage of passwords.

B. Definition(s)

- **Non-reversible format** – A reversible format stores a user name in a list with an associated password. When the user logs on this password is decrypted, the decrypted password is then compared to the password the user typed. A nonreversible format eliminates this weakness by performing a transformation on the password that makes it practically impossible to turn it back into the original password.
- **Passphrase** - A passphrase uses a series of words that may or may not include spaces; CorrectHorseBatteryStaple5 is the example passphrase. Although passphrases often contain more characters than passwords do, passphrases contain fewer “components” (four words instead of, say, 12 random characters).

- **User** – a.k.a "end user". Any individual who uses a computer or other information technology resource that is controlled, managed or owned by PennWest.

C. Policy

- PennWest Accounts created for users must use the following password policy. Password must be at least 12 characters in length.
- Password must be different than the previous 10 passwords.
- Password must have a minimum age of 0 days. (Your password can be changed immediately.)
- Password must have a maximum age of 365 days. (Your password expires every 365 days.)
- Password must contain at least 2 additional types of characters: Number, Capital Letter, or "Special Character" in addition to Lowercase Letters.

Passphrase – It is recommended that you use a passphrase which is a series of random words which may not include spaces. Example: CorrectHorseBatteryStaple5

Other Password Requirements

- Storage of Passwords
    - Passwords must be stored in a strongly encrypted format.
    - Passwords must be stored in a non-reversible format.
- Transmission of Passwords
    - For any new systems, passwords MUST be encrypted when transmitted on ANY type of network. For existing systems, passwords should be encrypted when transmitted on ANY type of network whenever possible.
- Account lock out provision
    - The University will disable user accounts for a period of time if there are repeated attempts to login with an invalid password.
    - Accounts will be locked out after the 10th invalid login attempt.
    - Lockout duration must be at least 15 minutes.
    - Account lockout counter will be reset after 15 minutes.
- Session Lock When Idle
    - The current user session will lock after 15 minutes of being idle (no user input) and the Session Lock login should be the same type as normal account login. Smart Classrooms, computer labs, and special use systems such as signage players may be excluded where a legitimate reason exists.
- Multi-Factor Authentication (MFA)
    - MFA will be used on all services that require authentication that support it.
        1. The Remember Me function will be set to 30 days (where supported).
- General
    - Users should not re-use University passwords for non-work related purposes. Ie Online Shopping, etc.
    - Users should never share their usernames, passwords, pin numbers or any other security related account information with anyone else.

- Exceptions will be granted on a case-by-case basis while carefully considering security and risk. Requests will be evaluated and approved by the CIO and Institution Leadership.

D. Procedure(s)

Not applicable.

E. Related policies

IT001: Acceptable Use Policy

F. Contact Information

Information Technology Services

G. Policy Review Schedule

All policies will be reviewed every two years or on an as needed basis if a change in BOG, PASSHE or Pennsylvania law would create the need for an immediate change.