University of Wisconsin-Platteville

Password Policy | Published: 01/26/2015
Section of: University Security Policies | Target Audience: Faculty, Staff, Students & Guests
PUBLIC | Page 1 of 4

University of Wisconsin-Platteville is hereinafter referred to as "the university."

1.0 Overview
A solid password policy is a critical security control for organizations to employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential for enabling security and compliance.

2.0 Purpose
The purpose of this policy is to specify guidelines for use of university passwords. Most importantly, this policy will outline why strong passwords are a necessity, and help individuals create passwords that are both secure and useable. Lastly, this policy will educate individuals on the secure use of passwords.

3.0 Scope
This policy applies to any person who is provided an account on the university’s network or systems, including: Faculty, staff, students, guests, contractors, partners, vendors, etc.

4.0 Policy

4.1 Construction
The best security against a password incident is simple: following a sound password construction strategy. The university mandates that users adhere to the following guidelines on password construction:

- Must be at least 8 characters long.
- Must be no more than 24 characters long.
- Must include at least 1 uppercase letter [A-Z].
- Must include at least 1 lowercase letter [a-z].
- Must include at least 1 number [0-9].
- NetID passwords MUST NOT contain any of the following:
  - Your first name, your last name, or your NetID.
  - The same character repeated more than 3 times consecutively.
  - A previously used password.
  - Parenthesis ( )
  - Minus sign (-)
- NOTE: Passwords are case sensitive
• NetID passwords will expire and must be changed every 180 days.

Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary

Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)

Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this way as well, for example an 'i' can be changed to a '!'.

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld'! Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

4.2 Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the organization's internal information. The following guidelines apply to the confidentiality of organization passwords:

• Users must not disclose their passwords to anyone
• Users must not share their passwords with others (co-workers, supervisors, family, etc.)
• Users must not write down their passwords and leave them unsecured
• Users must not check the "save password" box when authenticating to web applications
• Users must not send passwords via email
• Users must not re-use passwords
• Users should not use the same password for different systems and/or accounts
  o If you need to use your NetID for other UW-System applications, where possible, utilize a different password. If a non-UW application, if possible, utilize a user name and password combination different than your university NetID/password.

4.3 Change Frequency

In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum,
individuals using university resources must change their passwords every 180 days. The organization may use software that enforces this policy by expiring users' passwords after this time period.

4.4 Incident Reporting
Since compromise of a single password can have a catastrophic impact on network security and data integrity; it is the user’s responsibility to immediately report any suspicious activity involving his or her passwords to the IT helpdesk. If anyone requests your passwords over the phone or email, whether the request came from university personnel or not, should be rejected and immediately reported to the help desk. When a password is suspected to have been compromised the individual(s) will be required to change all his or her passwords.

4.5 Applicability of Other Policies
This document is part of the university’s cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the Assistant Vice Chancellor for Information Technology in consultation with Human Resources and/or the Dean of Students. Violations may result in disciplinary action, which, for students is outlined in Chapter 14 and Chapter 17 of the student conduct agreement and for all individuals may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of university property (physical or intellectual) are suspected, the university may report such activities to the applicable authorities.

6.0 Definitions

**Authentication** A security method used to verify the identity of a user and authorize access to a system or network.

**Password** A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

**Two Factor Authentication** A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History