Wabash College Password Policy

Version 1.1 • November 24, 2008

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in someone accessing your files and personal information, and could compromise Wabash College's entire data network. As such, all Wabash employees, students, and other authorized network users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Password Construction Requirements

Passwords on Wabash College computer systems must satisfy the following requirements:

1. Passwords must be at least 8 characters long.
2. Passwords must be changed at least once each year. The recommended change interval is six months.
3. Passwords may not be reused (you must choose a new password each time you change your password).
4. Passwords may not contain all or part of the username, or the person's name.
5. Passwords must meet at least **two** of the following criteria:
    a. The password contains a lowercase letter.
    b. The password contains an uppercase letter.
    c. The password contains a number.
    d. The password contains a special symbol from the set ~!@#$%^&*(){}[]<>

Password Construction Guidelines

Below are some additional tips for creating good passwords.

- Use long passwords. Each additional character increases the strength of the password many times.
- Use letters (both uppercase and lowercase), numbers, and symbols to form your password.
- Create a password that is complex but easy to remember by basing the password on a song, book title, quotation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- Don't use personal information that can be easily determined or guessed (your name or username, birthday or anniversary, family members' names, pets, phone number, street address, etc.).
- Don't use words in the dictionary, of any language.
- Don't use variations of Wabash, Little Giant, Wally, Monon Bell, or other Wabash words and phrases.
- Don't use sequences (12345, qwerty) or repeated characters (22222).

Password Protection Standards

Keeping your password safe is even more important than choosing a good password. Refer to the following guidelines to protect your password.

- Never give out your password through email or over the phone, regardless of who is asking for it. It is easy to spoof an email message to appear to come from the Wabash Help Desk. IT Services will never ask for your password over the phone or through email.
- Do not share your password with other Wabash people (or ask other people for their password), whether your boss, your administrative assistant, your co-workers, temporary replacement workers, student research assistants, classmates, pledge bothers, or friends. If you need to share files or other information, whether permanently or while you are on vacation or away from the office, contact the Help Desk and we can set up a secure way for you to share the information. If someone asks you for your password, refer them to this document or the Help Desk.
- Use a different password for off-campus systems (e.g. Facebook, Wabash Works, eBay, your personal ISP, banking and credit card sites, etc.). That way, if one password is compromised the other systems will still be safe.
- If you think your password may have been compromised, change your password and contact the Help Desk immediately.
- If you need to write down your passwords, keep the list in your wallet or purse, not next to your computer.

Changing Your Password

To change your Wabash password, go to:

https://www.wabash.edu/password

You must know your current password in order to change it. If you have forgotten your password, please contact the Help Desk for assistance (Baxter 33, x6400, helpdesk@wabash.edu). For security reasons, in most cases you will need to come to the Help Desk and show photo ID for us to change your password, but if that is not possible (e.g. you are studying off campus) we will collect other information to verify your identity.

As indicated previously, passwords expire after one year. Users whose password is about to expire will receive a daily reminder beginning one week before the password expiration date.

Datatel Password Requirements

Datatel users have a password for Datatel that is not synchronized with other campus systems. The same password construction requirements as described above apply to Datatel passwords, with the additional restriction that Datatel passwords must have at least two letters and one number or symbol in the first six characters of the password. To change your Datatel password, run **xpwd** from the Datatel menu.