**How to Change the Password to Your Lawrence Network Account**

**Applies To:** All Lawrence Staff and Faculty with a Lawrence Issued Device

Your Lawrence password will expire once a year. You can change it more often than that if you are concerned that it may have been compromised or if you are instructed by Lawrence IT to change it. Creating a strong password is essential for protecting your accounts and sensitive information. Follow these guidelines to ensure your password meets security best practices.

It will take about 15 minutes for the new password to synchronize across all your devices (such as between a laptop and your phone)

To ensure your privacy and the security of Lawrence University, never share your password. Technology Services and the helpdesk will NEVER ask for your password via email.

**How to Reset Your Password if you have a Windows Device:**

- Go to the link: aka.ms/sspr
    - If you need additional help with the self-service password reset tool, click here.
- You'll be directed to a screen where you will enter your [username]@lawrence.edu and the characters for the Captcha. Please note: You might have to try the Captcha more than once.
- You'll then be directed to the screen for Multi-Factor Authentication using the email, mobile phone, and/or Authenticator app.
- Once both methods have been verified, you'll be directed to change your password – see below for password guidelines.

You may also contact the Help Desk for assistance.

**How to Reset Your Password if you have an Apple Device:**

Note that it is a two-step process to change your password on an Apple device. First you change the password for the Lawrence network. Next you will also need to update your password locally on your Apple device. Until this is done, you may run into situations where your old password is recognized rather than your new one.

- Make sure you are on a wired or docked connection (not wifi)
- Go to the link: aka.ms/sspr
- You'll be directed to a screen where you will enter your [username]@lawrence.edu and the characters for the Captcha. Please note: You might have to try the Captcha more than once.
- You'll then be directed to the screen for Multi-Factor Authentication using the email, mobile phone, and/or Authenticator app.

- Once both methods have been verified, you'll be directed to change your password – see below for password guidelines.
- Contact the IT Help Desk for assistance updating your local keychain password. Until you do, you may run into some situations (like FileVault and KeyChain) where your old password is recognized rather than your new one.

You may also contact the Help Desk for assistance.

**Password Guidelines and Best Practices**

Your password **must** meet the following criteria:

✅ **Minimum length:** 14 characters
✅ **Character requirements:** Must include at least three of the following four categories:
- Uppercase letters (A–Z)
- Lowercase letters (a–z)
- Numbers (0–9)
- Special characters (e.g., !, $, #, %)

✅ **Should not contain:**
- Your name or username
- Personally identifiable information (PII), or information easily found on the internet and social media
- Spaces
- A password you've previously used

✅ **Additional restrictions:**
- Passwords cannot be changed more than once in a 24-hour period.

**Current Best Practices (Based on CISA & NIST Guidelines)**

- **Use passphrases instead of complex passwords:** A strong passphrase is a sequence of random words or a sentence that is easy to remember but hard to guess (e.g., **"OrangeRiver$LaptopBlue"**).
- **Avoid password reuse:** Never use the same password across multiple accounts. If one account is compromised, others will be at risk.
- **Use a password manager:** A password manager like KeePass can securely generate, store, and manage unique passwords for each of your accounts.
- **Enable multi-factor authentication (MFA):** Whenever possible, use MFA for an extra layer of security.
- **Monitor for breaches:** Use tools like Have I Been Pwned (https://haveibeenpwned.com) to check if your credentials have been exposed in a data breach. If they have, consider changing all your passwords.

By following these guidelines, you can improve security while making password management easier.