1. **New User Setup**

From your web browser, visit https://password.umsystem.edu/newusersetup/.

- Enter your University username/also known as pawprint, or SSO ID. (For the rest of the instructions, we will refer to it as username). Click submit.
- Enter your information in the following fields: Mobile/alternate phone (for text), work/home phone, external/non-University email (alternate address).
  - Username, First Name, Last Name, and primary/University email are pre-populated.
- To complete new user setup, you must answer 3 knowledge based questions (the 3rd question/answer combination is for Help Desk verification purposes). If you would like to change a question option, use the pull down menu on the question field and select from a new set of pre-approved questions.
- Once you have answered all 3 questions, click update.
- You will receive an email stating your account has been updated. Your browser will redirect you to the New User Password Setup page.

**Password Setup:**

- Enter your University username.
- You are prompted to choose a delivery method for your passcode.
  - Options include:
    - Phone/mobile: Voice or SMS/text
    - Email
    - Send login request to <device name>*
    - Send passcode to <device name>*
- Select your preferred delivery option:
  - If you choose mobile SMS/text, you will receive your passcode via text message.
  - If you choose voice, you will receive your passcode via phone call.
  - If you choose email, you will receive your passcode to your pre-set email account.
  - If you choose Send Login Request to <device name>, you will receive a Login Request notification on your device within the SecureAuth application (a notice may also appear in your device's Notification Center, depending on the notification settings you have setup. Notification Center message will be from Authenticate and will read: Login Request. Tap to see request in app).
    - Request screen states: U of Missouri then the name of the tool you made the request from (i.e. forgot password or password reset). Next line: User name, date/timestamp, and City/Country.
    - You are given the option the Accept or Deny. Click accept. Accept is acknowledged and your web browser takes you immediately into the password tool. (You skip the passcode prompt steps below).
- If you choose send passcode to <device name>, you will receive a notification within the SecureAuth app.
  - Message will read: SecureAuth. Your one time password is ------ ,<your name>. (A notice may also appear in your device’s Notification Center, depending on the notification settings you have
setup. Notification Center message will be from Authenticate and will read: Your one time password is ------, <your name>.

- If you choose Time-based Passcode-SecureAuth OTP Mobile App, you will need to access the app.
  - You must enter the PIN you setup during the application installation/registration.
    - You will be presented with your time sensitive passcode ------. (Passcodes will continue to update until you close the app).
- You will be prompted to enter the passcode in your web browser. Type the passcode in the field and click submit.
- On the password setup screen, you are provided your username for confirmation. Complete the new password field and the confirm password field by following the password requirements. Click submit.
- Once successful, you will be presented with the following message in your browser window: Password has been successfully changed.
- You will receive an email notifying you that your password has been changed.

Log in to library.muhealth.org
Enter your user name and password into the proxy server window to access library resources
(AccessMedicine, CIHAHL, ClinicalKey, DynaMed, MEDLINE (Ovid), Micromedex, PubMed, Scopus, Up to Date and Web of Science)

If you experience problems with the above process, please call 573-882-5000 or visit https://doit.missouri.edu/tech-support/.