Wharton Passwords: Guidelines and Tips

This article outlines tips and guidelines for creating passwords for both PennKey and Wharton. Both accounts share the same password requirements.

To change your password, see Change / Reset Password.

NOTE - To help take the burden of complex passwords off of your shoulders, Wharton offers access to an encrypted password manager called LastPass. Find out more about how it works and how to sign up.

Wharton Password Guidelines

Password Length

Your Wharton password must meet differing requirements, depending on length:

<table>
<thead>
<tr>
<th>Password Length</th>
<th>Requirements</th>
<th>Example (Do NOT use these for your actual password.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20+ Characters</td>
<td>Any US keyboard characters.</td>
<td>boldaugustpretzelcloud</td>
</tr>
<tr>
<td>16-19 Characters</td>
<td>Upper and lower-case letters</td>
<td>BoldAugustPretzel</td>
</tr>
<tr>
<td>12-15 Characters</td>
<td>Upper and lower-case letters and numbers</td>
<td>4Bold7August8</td>
</tr>
<tr>
<td>8-11 Characters</td>
<td>Upper and lower-case letters, numbers and symbols</td>
<td>$4Bold78!</td>
</tr>
</tbody>
</table>

Things you can't use as your password:
- Easily guessed or known compromised passwords (example: 12345678).
- Your PennNet ID, username (even backwards), and your first, middle, or last name.
- Single dictionary words, even if they meet the length requirements.

Refresh Your Password Frequently

You should change your password every 90-120 days (3-4 months).

Enable MultiFactor Authentication

Whenever possible you should enable multifactor authentication. Also known as "two-step verification", this will
Tips for Creating a Password

Your password should be easy for you to remember, but should not make sense to anyone else.

- Avoid basing your password on your personal information like your birthday, phone number, address, or other personal information that may be publicly available.
- String together four or more unrelated words for a long, secure password.
- Replace letters with numbers that look similar to make an easy to remember yet strong password.
  - For example, turn "Wireless" into "W1r3l3ss" or "learning" into "13arn1ng"