PennKey Password Rules

To protect your personal files and Penn resources, your PennKey password needs enough length, variety, and unpredictability to qualify as secure.

The simplest option is a password whose length alone makes it resistant to being compromised. Long passwords have fewer requirements.

Tip: Use four or more unrelated words to form a strong password that’s easy to remember, such as: boldaugustpretzelcloud

You can also create a shorter password that introduces more variety and unpredictability into your character combination. A password this long must contain:

<table>
<thead>
<tr>
<th>20+ characters</th>
<th>any character type</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 - 19 characters</td>
<td>A a</td>
</tr>
<tr>
<td>12 - 15 characters</td>
<td>9 A a</td>
</tr>
<tr>
<td>8 - 11 characters</td>
<td>? 9 A a</td>
</tr>
</tbody>
</table>

20 or more characters: any U.S. keyboard characters
example: boldaugustpretzelcloud

16-19: capital and lower-case letters
example: BoldAugustPretzel

12-15: capital and lower-case letters and numbers
example: 4Bold7August8

8-11: capital and lower-case letters, numbers, and symbols
example: $4Bold78!

PennKey passwords are also screened for easily guessed combinations, such as:
• Portions of, or simple variations on, your name or username
• Single dictionary words (English and non-English): Diversifications, Alternativamente
• Common 2-3 word combinations: PhiladelphiaEagles
• Predictable strings: 123123, abcdef, qwerty, johnpaulgeorgeringo, pa$$w0rd, drowssap
• Compromised passwords on published lists

If you have trouble remembering a longer password, write it down and handle it with the same caution you would a credit card.