Name: Amber Radune

Class: CYBR-1100
Date: 8-29-2025

Case Project 2-2: Password Requirements

These are the three password requirements that are the weakest.

1. **MoviePass**

   Requirement: “Passwords should be between 5 & 20 characters.”
   That’s way too weak—having only five characters is way too short to be safe. Even the maximum they allow isn’t great, and a password that short could be guessed by brute force really fast. A better option would be to have at least 12 characters, giving people room to go up to something like 64 if they want, and let them use letters, numbers, and symbols so they can create stronger yet easy-to-remember passwords.

2. **Blue Shield of California**

   Requirement (contradictory): It states that the password must include at least 3 of the following: uppercase, lowercase, numbers, or symbols, but then it also specifies that symbols cannot be used. That makes no sense because you can’t follow both rules at the same time. It’s just confusing and would cause people to keep failing when they try to make a password. A better approach would be to allow people to use all options, uppercase, lowercase, numbers, and symbols, and simply recommend that they use at least three of these types. That way it’s clear, flexible, and actually makes sense.

3. **Southern Illinois University, Edwardsville**

   Requirement: Passwords must be 7–8 characters, at least five unique characters, include one letter and one number, start with a letter or number, exclude many symbols, avoid dictionary words (even backward), prevent patterns, and disallow National Insurance number format.
   This policy is overly complicated; it only allows 7–8 characters and imposes numerous random rules, making it almost impossible to create a valid password. Most of those restrictions don’t even make it more secure. A better approach would be to require at least 12 characters (with no caps, or something reasonable like 64), ensure there’s at least one letter and one number, allow people to use symbols if they want, and block only really weak or known compromised passwords. There’s no need for weird rules like “no backward words” or “no repeating patterns.” They just annoy users without really improving security.

Summary Paragraph

Some of the worst password rules I saw were MoviePass's requirement of only five characters, Blue Shield's confusing instructions about symbols, and Southern Illinois University's overly complicated password policy that’s almost impossible to follow. Rules like that don’t actually make accounts safer—they just frustrate people. A better approach is to focus on using longer passwords, such as at least 12 characters, while still providing flexibility in how people create them. That way, users can create easy-to-remember passphrases instead of struggling with restrictive rules. It keeps things more secure but also realistic for everyday users.