Colorado Department of Public Health and Environment
Strong Password/Passphrase Guidelines

Strong passwords are necessary to ensure passwords cannot be broken. Weak passwords may be guessed or are likely to be broken with "dictionary" software that looks for standard words and names.

Strong passwords are easier to remember if they are real phrases:

- Must be at least 8 characters in length, but ideal is at least 20 characters
- Have mixed case: some capitals and some lowercase letters
- Have at least one number
- Have a special character
- Are not incremented with each change (Quarter1, Quarter2, etc.)
- Are not reused
- Must be changed periodically

There are tricks to creating strong passphrases that still are easy to remember. Below are some suggestions for how to construct your own strong passwords. Think through your own approach, and you will find that it is not so difficult to remember even strong passwords.

1. Pick a **phrase** that is at least 8 characters long, preferably at least 20 characters in length. It can be a line from a song, a statement about something you like or hate, or anything that is meaningful to you and that you can remember.
2. Remove the spaces between words, and change some words to "shorthand" like that used in text messaging: four or for=4, you=u, etc.
3. Change some letters to special characters. For instance, a=@. Capitalize a letter…it does not have to be at the beginning of the word. If you are going to use the shift key for a special character, why not keep it down to capitalize a letter either before or after the special character? Examples:
    - Iwishu@M3rryChristmas
    - mydogBiscuitneeds2get@life
    - 2beornot2beTH@tisthe?
    - myh0meiswheremyHE@rtis

To test the strength of a password *similar* to yours, visit https://www.microsoft.com/security/pc-security/password-checker.aspx.