STRONGER PASSWORDS, STRONGER SECURITY

It's important to create strong, complex passwords for your systems. That's why we've put together these best methods for stronger passwords to help you train your employees. Keep in mind, though, that based on the risk of each system, these standards may fluctuate.

- Create passphrases instead of passwords. Individual words, even with slight variations, are easy to guess, but a series of words in a passphrase make them more secure.
- Consider making the passphrase or password longer than the minimum limit. Longer passphrases are harder to break than shorter, complex passwords. Longer passphrases could also be used to relax other complexity or frequency of change requirements.
- For a non-privileged account, your complex password should be at least 12 characters long and should be updated every 90 days. Privileged account, the password should be at least 14 characters and should be updated every 45 days.
    - User accounts should be temporarily disabled if more than 5 failed attempts are detected.
- If available, use multi-factor authentication.
- Do not use the same password for multiple systems, websites, or accounts.
- Do not use single words that can be found in the dictionary of any language. Password-cracking tools often come with dictionary lists that can try thousands of common words.
- Do not use passwords that include personal information that could be easily accessed or guessed. This includes your birth date, your Social Security or phone number, or names of family members.
- If you need help managing your passwords, do not store your list of passwords in a plain text file on your computer. Instead, there are several third-party programs that can help you stay secure, including LastPass, DashLane, 1Password, Roboform, PasswordSafe, or Keepass.

sales@sbscyber.com | 605-923-8722 | www.sbscyber.com