Password Construction Guidelines

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides Campbell County's requirements for creating secure passwords.

2. Purpose

The purpose of this guidelines is to provide the current requirements for the creation of strong passwords.

3. Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, and local/remote appliance logins.

4. Statement of Guidelines

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 8 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "*I can't wait for summer*" or "*yellow-pad-hot-water*". Passphrases are both easy to remember and type yet meet the strength requirements. Please see our password requirements listed below:

- *Be at least eight (8) characters in length*
- *Contain characters from these categories:*
  - *Uppercase characters (A through Z)*
  - *Lowercase characters (a through z)*
  - *Numbers (0 through 9) or non-alphabetic special characters (for example,!, $, #, %)*
- *Not contain the user's account name or parts of the user's full name that meet or exceed three consecutive characters*
- *Not be a recycled password (i.e., a password used previously)*

In addition, every work account should have a different, unique password. To help users manage multiple passwords securely, we highly encourage the use of an authorized 'password manager' software, which should include options for hardware-based or biometric authentication for added

protection. Whenever possible, also enable multi-factor authentication (MFA) for an extra layer of security.

5. Policy Compliance

5.1 Compliance Measurement

The Information Technology Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the IT Department in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to in-person password remediation.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
August 2018	Jonathan Pingilley	Adopted from SANs Security Policy Project
January 2025	Jonathan Pingilley Jodi Crews	Updated areas to reflect new technologies and policies