Title VI – Information Services
SECTION 466 –PASSWORD POLICY

Latest Update: June 2024

A. OVERVIEW

Strong passwords are essential for maintaining computer security. They are one of the front-line defenses of protection for user accounts. A poorly chosen password may result in a compromise of the County of Santa Cruz's entire network. As such, all account holders (including staff, contractors, and vendors with access to the County's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

B. PURPOSE

The purpose of this policy is to establish a standard for creating strong passwords, the protection of those passwords, and the frequency at which account passwords must be changed.

C. SCOPE

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that has access to the network, or systems that are used in the normal course of business of the County, whether residing at the County or hosted.

D. POLICY

1. General
   - All user passwords must expire within a prescribed amount of time based on the guidelines below.
   - Passwords must conform, where necessary, to the appropriate regulatory and legal requirements for system access such as defined by CJIS, IRS and DMV security requirements.
   - Where possible, multifactor authentication should be used to further secure accounts.
   - Multifactor authentication is required to access all Microsoft applications and services
   - Passwords must be temporarily locked out after no more than six (6) invalid access attempts and remain locked out for a minimum of thirty (30) minutes or until reset by a system or account administrator.
   - All systems shall protect passwords with strong encryption during transmission and storage.
   - All employees are accountable for all activities performed under their account unless an investigation proves that the employee did not violate policy at the time.
   - All vendor-supplied default passwords must be changed before the system is used for County business.

- Employees shall not allow others to access a system while it is logged on under their credentials. The only exception is when the business needs of a County department require an alternative login practice for specified functions, such as remote support.

2. Guidelines for Password Construction requirements
   - Be a minimum of twelve (12) characters on all systems
   - Not be a single dictionary word or proper name
   - Not contain the user ID
   - Expire within a maximum of calendar 90 days
   - Not be identical to the previous twelve (12) passwords
   - Contain alphanumeric character and special characters
   - Account will lock out after 6 incorrect password attempts

3. Password Protection Standards

All passwords are to be treated as sensitive, confidential information

- Do not send a password in an email, text, or any electronic messaging system
- Do not share your password with anyone
- Do not write down passwords or leave them accessible to others
- Do not use the “remember password” feature in web browsers
- Do not store your passwords on any computer system in plaintext or unencrypted
- Do not reveal your password on questionnaires or security forms

If someone demands a password, refer them to this policy or have them contact the CISO for the Information Services Department for the County of Santa Cruz.

If an account or password is suspected to have been compromised, report the incident to the IT Support desk and immediately change all passwords.

E. PENALTY

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Resources:

DHCS and CDSS Privacy and Security Agreements
Department of Motor Vehicles Information Security Agreement
Criminal Justice Information Services Security Policy, U.S Department of Justice
Payment Card Industry Data Security Standards (PCI-DSS)
County of Santa Cruz Acceptable Use Policy