# PASSWORD POLICY

## I. INTRODUCTION

Users at the San Diego Workforce Partnership, AJCC Network, and Subrecipients must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of SDWP's strategy to make sure only authorized people can access these resources and data.

All employees who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorized people. Passwords are a first line of protection against any unauthorized access into your personal computer. The stronger the password, the higher level of protection your computer has from malicious software and hackers.

The purpose of this policy is to make sure all SDWP resources and data receive adequate password protection. The policy covers all users who are responsible for one or more account or have access to any resource that requires a password.

### A. PASSWORD CREATION

- All passwords should be reasonably complex and difficult for unauthorized people to guess.
  - Passwords should be at least 8 characters and be a combination of 3 of the following 4 items:
    - Uppercase characters (26 letters A-Z)
    - Lowercase characters (26 letters a-z)
    - Numbers (numbers 0-9)
    - Punctuation Marks and other Special Characters (for example: ~!@#$%^&,./?<>)
  - These requirements will be enforced with software when possible.
- In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective.
- A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember" can become "TmB0WTr!".
- Employees must choose unique passwords for all of their company accounts and may not use a password that they are already using for a personal account.
- All passwords must be changed regularly, at least every 90 days.
- If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.
- Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.
- Password history should also be enforced to prevent users from reusing the same passwords.

### B. PROTECTING PASSWORDS

- Account lockouts should be implemented to limit the number of times an incorrect password can be entered.
- Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.
- Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.
- Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All employees will receive training on how to recognize these attacks.
- Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

- Employees may not use password managers or other tools to help store and remember passwords without IT's permission.