**Sacramento Employment and Training Agency**

**Password Policy**

**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. These guidelines provide best practices for creating secure passwords.

**Purpose**

The purpose of these guidelines is to establish a standard for creation of strong passwords and the protection of those passwords.

**Scope**

These guidelines apply to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. These guidelines apply to all user-level account passwords that are associated with systems that are directly managed by SETA.

**Password Construction Guidelines**

Strong passwords are long; the more characters you have the stronger the password. **Passwords are required to be a minimum of 10 characters in length**. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include “*It’s time for vacation*” or “*block-curious-sunny-leaves*”. Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics and should not be used:

* Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
* Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
* Are some version of “Welcome123” “Password123” “Changeme123”

**Password Protection Guidelines**

1. Password Creation
   1. All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
   2. Users may not use any work related passwords for their own, personal accounts.
2. Password Change
   1. Passwords should be changed only when there is reason to believe a password has been compromised.
   2. Password cracking or guessing may be performed on a periodic or random basis by the IT Team or its assigned vendor. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.
3. Password Protection
   1. Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential SETA information.
   2. Users must not send passwords in email messages, or any other form of electronic communication, nor reveal over the phone to anyone.
   3. Do not use the “Remember Password” feature of applications (for example, web browsers).
   4. Any user suspecting that their password may have been compromised must report the incident to the IT HelpDesk and change all passwords.
4. Application Development

Application developers must ensure that their programs contain the following security precautions:

* 1. Applications must support authentication of individual users, not groups.
  2. Applications must not store passwords in clear text or in any easily reversible form.
  3. Applications must not transmit passwords in clear text over the network.
  4. Applications must provide for some sort of role management; such that one user can take over the functions of another without having to know the other's password.

**Policy Compliance**

1. Compliance Measurement

The IT Team will verify compliance to this policy through various methods, which could include but not be limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the Agency management.

1. Exceptions

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