

Password Procedures

Passwords are an important aspect of information security. A poorly chosen password may result in unauthorized access and/or exploitation of SDCOE's resources. All users, including contractors and vendors with access to San Diego County Office of Education systems and networks are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1. Purpose

The purpose of this procedure is to communicate the standard for strong passwords, the protection of those passwords, and the frequency of change.

2. Scope

The scope of this procedure 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 resides at any San Diego County Office of Education facilities, has access to the SDCOE network, or stores any non-public SDCOE information on premise or in the cloud. Employees, contractors, and temporary staff must follow all SDCOE password procedures.

3. Procedure

3.1 Password Creation

- All user-level and system-level passwords must conform to the *Password Construction Guidelines* (see below).
- Users must not use the same password for SDCOE accounts as for other non-SDCOE access (for example, personal ISP account, option trading, benefits, and so on).
- Where possible, users must not use the same password for various SDCOE access needs.
- User accounts that have elevated privileges must have a unique password from all other accounts held by that user.

3.2 Password Change

- All passwords for user accounts with elevated privileges (for example, root, enable, NT admin, application administration accounts, and so on) must be changed at least every six months.
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least once a year. The recommended change interval is every six months.
- Password cracking or guessing may be performed on a periodic or random basis by the Security Team or its delegates. 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.

3.3 Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential SDCOE information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be left on answering machines, it should be shared with the intended person only.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").

- Do not share SDCOE passwords with anyone (superior, peer or subordinate) under any circumstances.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption. Refer to SDCOE encryption procedure for help on encrypting password files.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

3.4 Application Development

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

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- 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. This functionality should be limited to Admin users of the system and should be approved by system owner and documented.

3.5 Use of Passwords and Passphrases

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "U Mu5t B the Ch@nge U W!5h 2 C !n the W0rld"

All of the rules above that apply to passwords also apply to passphrases.

3.6 Password Construction Guidelines

SDCOE requires a strong password that meets the following criteria:

- It must be a minimum of ten characters
- It must contain three of the following types of characters:
 - Uppercase letter
 - Lowercase letter
 - Numeral
 - Non-alphanumeric characters (for example %, !, &, #, \$, @, ^, *, (,), _ , - , + , =)
- It cannot contain a user's logon name
- It cannot contain any portion of the user's full name

4. Compliance

The Integrated Technology Services team will verify compliance to this procedure through various methods, including but not limited to, business tool reports, internal and external audits, and device monitoring. ITS reserves the right to prevent the transfer of data it finds unsecure. ITS will engage in such action if it finds that the data is being used in such a way that puts the SDCOE or its employees at risk.

All users agree to immediately report to his/her manager and SDCOE ITS, if they observe any deviation from the procedures mentioned above.

5. Exceptions

Exceptions to this procedure may be requested on a case-by-case basis and must be approved in advance by the Assistant Superintendent of Integrated Technology Services.

6. Procedure Non-Compliance or Deviation

Failure to comply with the password procedures may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

7. Revision History

Responsible	Date of Change	Summary of Change