User Password Guidelines

Southwest Area Technology Team Collaborative Draft Policy Template

1. Purpose

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the District's entire school network. As such, all District employees (including contractors and vendors with access to the District's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Guidelines

The purpose of these guidelines is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. 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 resides at any District facility, has access to the District network, or stores any non-public District information.

3. Procedure

3.1. General:

3.1.1. All admin-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least every 3 months.

3.1.2 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

3.1.3 User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

3.1.4 Passwords must not be inserted into email messages or other forms of electronic communication.

3.1.5 All user-level and system-level passwords must conform to the guidelines described below.

3.2. Guidelines:

3.2.1 General Password Construction Guidelines

Passwords are used for various purposes in the District. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection and voicemail passwords. All users should select strong passwords.

Examples of poor, weak, or easy to break passwords include:

- A password that contains less than eight (8) characters
- A password that uses only alphabetic characters
- A password that is a word found in a dictionary (English or foreign)
- A password that is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "<District Name>", "<School Name>", "<City>" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Simple word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~- =\`{}[]:";'<>?,./)
- Are at least eight (8) alphanumeric characters long and use a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Passwords should be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

3.2.2. Password Protection Standards

3.2.2.1 Do not use the same password for District accounts as for other non-District access (e.g., personal ISP account, option trading, benefits, etc.).

Where possible, don't use the same password for various District access needs. For example, select one password for the Grading and Student Information systems (SIS) and a separate password for Web and Email systems.
3.2.2.2 Do not share District passwords with anyone, including administrative assistants or secretaries.
3.2.2.3 All passwords are to be treated as sensitive, confidential District information.
3.2.2.4 Users of <District> computers will not:

- reveal a password over the phone to ANYONE unless a known identity is established
- allow others to access your computer or the District computer systems using your password
- share any private passwords with students
- reveal a password in an email message
- reveal a password to supervisors unless specifically directed to do so by an employment directive
- talk about a password in front of others
- hint at the format of a password (e.g., "my family name")
- reveal a password on questionnaires or security forms
- share a password with family members
- reveal a password to co-workers while on vacation

3.2.2.5 If a person demands a password, refer the person to this document or have the person call someone in the Information Security Department.
3.2.2.6 Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, Firefox, Messenger).
3.2.2.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including electronic organizers or similar devices) without encryption.
3.2.2.8 Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.
3.2.2.9 If an account or password is suspected to have been compromised, report the incident to the District Technology Coordinator and change all passwords.

3.2.3 Passphrases

- Passphrases are generally used for public/private key authentication. Without the passphrase to "unlock" the private key, the user cannot gain access.
- 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" where words in a dictionary are randomly and repeatedly tried until the correct password is found.
- 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:
- "The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"
- All of the rules above that apply to passwords apply to passphrases.