De Soto School District 73

Password Administrative Policy

1.0 PURPOSE

This policy describes the requirements for acceptable password selection and maintenance to maximize security of the password and minimize its misuse or theft. Passwords are the most frequently utilized form of authentication for accessing computer resources. The proliferation of automated password-cracking programs and the activity of malicious hackers and spammers exponentially increase security risks when using weak passwords. Therefore, password use must adhere to the policy statement found below.

2.0 SCOPE

This policy applies to anyone (employees, students, interns, contractors, etc...) accessing or utilizing the network, computers, or data. This use may include, but is not limited to, the following: computers, laptops, district-issued phones, and hand-held form factor computing devices (e.g., USB memory keys, electronic organizers), as well as electronic services, systems and servers. This policy covers departmental resources as well as resources managed centrally.

3.0 POLICY

All passwords (e.g., email, web, desktop computer, etc.) should be strong passwords and follow the standards listed in this policy. In general, a password's strength will increase with length, complexity and frequency of changes.

Greater risks require a heightened level of protection. High risk systems include but are not limited to systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

All employees, interns, and contractors are expected to set a good example through a consistent practice of sound security procedures.

1. All passwords must meet the following minimum standards:
    a. Be at least eight (8) alphanumeric characters long.
    b. Contain at least one digit or punctuation character as well as letters (e.g., 0-9, ~`!@#$%()_-'{.})
    c. Contain both upper and lower case characters (e.g., a-z, A-Z).
    d. Not be a word in any dictionary, language, slang, dialect, jargon, etc.
    e. Not be based solely on easily guessed personal information, names of family members, pets, etc.
    f. Password history is enforced. The last five (5) passwords are remembered.
    g. The minimum password age is five (5) days.

2. Account lockout policies
    a. Account lockout duration: 10 minutes
    b. Account lockout threshold: 5 invalid logon attempts
    c. Reset account lockout counter after: 10 minutes

3. To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must never be used as a user ID or a password.
4. All passwords are to be treated as sensitive information and should therefore never be written down or stored on-line unless adequately secured. NOTE: Do not use the password storage feature offered on Windows or other operating systems.
5. Passwords should not be inserted into email messages or other forms of electronic communication without encryption.
6. The same password should not be used for external or personal access needs (e.g., online banking, personal email, benefits, etc.).
7. Employee passwords must be changed every 90 days, or sooner, and must meet complexity requirements.
8. Student passwords must meet password length and complexity requirements.
9. Individual passwords should not be shared with anyone, including administrative assistants or administrators. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those passwords, and that person will ensure that only appropriately authorized employees have access to the passwords.
10. If a password is suspected to have been compromised, it should be changed immediately and the incident reported to the IT Department as soon as possible.

4.0 POOR PASSWORD CHARACTERISTICS

- The password contains fewer than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is common usage words such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software, etc.
- Words including any part of your organization or department name, city, state, zip, or any derivation.
- Birthdays and other personal information such as address and phone numbers.
- Word or numbers patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by digit (e.g., secret1, 1secret) Note: These passwords are easy to crack.

5.0 STRATEGIES FOR CHOOSING A GOOD PASSWORD

- Use lines from a childhood verse:
  Verse Line: Yankee Doodle went to town
  Password: YDwto#town
- Pick letters from a phrase that's meaningful to you:
  Pass Phrase: Do you know the way to San Jose?
  Password: D!Y!KtwTSJ?
- City Expression interspersed with street address:
  Chicago is my kind of town
  Password: C1i2mY1K5o6t

Note: You shouldn't use any of the passwords used as examples in this document. Treat these examples as guidelines only.