Network Password Policy and Guidelines

Overview

AISD employees and students can access district applications and data from anywhere in the world with a computer and internet connection. Because strong and secure passwords help ensure the security and integrity of AISD applications and information, AISD employees, students, contractors, and vendors are responsible to securing their passwords as described below.

Purpose

The purpose of this policy is to establish a standard for creating strong passwords, securing them, and outlining the frequency these passwords should be changed.

Scope

This policy applies to AISD employees, students, vendors, and staff that logon to the AISD network.

Policy Statement

All AISD users must adhere to account password standards, take reasonable measures to protect their accounts and passwords, and are required to change their passwords on a regular basis.

Password Standards

- Any password should be changed immediately if it has been compromised.
- Individual employee and student network account passwords should be changed every 180 days.
- Passwords for applications that are not tied to MS Active Directory should be changed every 180 days as well.
- The passwords for generic accounts should be changed at least once a year.
- Passwords to the <School> Sub and <School> Guest account (e.g., Sub Anderson, Guest Anderson) will be changed every 30 days.
- Vendor and System Account passwords need to be changed at least once a year. The passwords should be very strong, kept secure, and changed immediately if there is a chance unauthorized personnel have compromised the account.

Password Guidelines

When possible, AISD recommends the following the guidelines below to select a secure password:

- Make it least 8 characters long and use a passphrase
- Include upper and lower case characters (e.g., a-z, A-Z)
- Include both numbers and special characters (e.g., 0-9, ~, @, #, $, %, ^, &, *, (, ),=, +, ;, :, ', "", <, >, >, ?.

Page 1 of 3
• Do not be a single word found in the dictionary
• Do not include words associated with the school or district (e.g., mascots, school name, school colors)
• Do not make it a person, place, or thing.
• Do not include personal information (e.g., names of spouses, children, grandchildren, or pets; birthdays; or anniversaries.)
• Do not make it a repeating pattern when you change it so that the first part of the password remains the same but just a number or character is changed at the end of the password (e.g., MyDogHasFleas001 to MyDogHasFleas002.)
• Do not use a keyboard pattern such as qwerty or 12345678.

A passphrase is a phrase that you use as a password, but its length makes it more secure. For example, if you enjoy playing volleyball, a good password might be 1MeanSpikeQueen!.

If you are a Dallas Stars hockey fan, a good password might be ILoveJussiJokinen#36.

If you are a Dallas Cowboy fan, you might make your password an acronym of the phrase I Hope The Dallas Cowboys Win Super Bowl #68!, which would be IHtDCWSB#68!.

If your dog Spike chases squirrels, you might pick MyD0gSpikeHates@llSquirrels or you could use the acronym of that phrase with a couple of numbers at the end to make it 8 characters: MDSH@S11

Computers should not be unattended with the user logged on and no password protected screen-saver active.

When a user is logged in to a computer, but must leave it unattended, the user should lock their computer until they return. Users can press the CTRL-ALT-DEL keys and select "Lock Computer" (On certain computers, password protected screen savers are enabled and should protect the computer within 30 to 60 minutes of user inactivity).

Here are some video guidelines on how to select a strong password: http://www.freetech4teachers.com/2013/05/5-videos-about-crafting-strong-passwords.html#.UYen7spPzKU

Password Requirements

The following password requirements will be set by the IT department:

1. Minimum Length - 5 characters
2. Passwords are case sensitive
3. Password history - Require a number of unique passwords before an old password may be reused. This number must be no less than 8.
Allen ISD

Network Password Policy and Guidelines

Technology Department

Revision Date: 05/23/2013

4. Maximum password age - 180 days

5. Account lockout threshold – 6 failed login attempts

6. Reset account lockout after – 3 minutes. The time it takes between bad login attempts before the count of bad login attempts is cleared. If there are six bad attempts in 3 minutes, the account would be locked.

7. Account lockout duration – 5 minutes

Password Protection Guidelines

In order to keep your password from falling into the wrong hands, please follow these guidelines:

- Do not make your Allen ISD network password the same as the one you for your personal accounts (e.g., personal e-mail, on-line banking, social medial.)
- Do not share your password with anyone, including students, substitutes, co-workers, supervisors or family members.
- Do not reveal your password over the phone to anyone.
- Do send your password in e-mail to anyone.
- Do not post passwords on computers, whiteboards, etc. . . .
- Do not give your password to co-workers when on vacation.
- Do not use the “Remember Password” feature on browsers or other applications.
- Change your password immediately if you think it may have been compromised.
- If you must write down a password, kept in in a locked drawer at all times.
- Be careful about letting someone see you type your password.

If someone demands to know your password, please refer him to this document or have him call the AISD Technology Department.

Changing Passwords

When logging into computers, users will receive a message stating their password is about to expire at least a week before their password expiration date. At any time, the user may change their network password on district computers by pressing CTRL+ALT+DELETE, and then clicking Change a password. Users may also change their password from the Citrix web interface at https://tr.allenisd.org

If the password to a network account is forgotten, staff and students should visit with their campus tech in order to have their password reset. If the campus tech is not available, the user must visit the Technology office and present a photo ID in order to have their password reset.

Enforcement

Failure to secure your network password may result in applicable legal action and disciplinary action up to termination of employment.