City of Frisco Personnel Policies
Password Policy

Topic: Password Policy Approved by Ordinance # 2021-07-46

Effective Date: Feb. 11, 2008

Revision Date: 07/06/2021

Overview

In conjunction with the City of Frisco's ("City's") Acceptable Use Policy, the following policy applies to the use of passwords. 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 City's entire network. As such, all City employees (including contractors and vendors with access to city systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

This policy applies to all employees, contractors or volunteers of the City who have, or are responsible for, a computer account, or any form of access that supports or requires a password, on any system that resides at any City facility, has access to the City network, or stores any public or non-public City information.

Policy

General

1. Passwords must be changed every 365 days.
2. Passwords must be changed immediately if it is suspected the password has been compromised.
3. The last 10 passwords cannot be re-used.

Password Construction Requirements

Passwords are used to access any number of City systems, including the network, e-mail, the Web, and voicemail. Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

1. Passwords must contain at least 20 (twenty) characters.
2. Passwords must not be based on a users' personal information or that of his or her friends, family members, or pets. Personal information includes logon I.D., name, birthday, address, phone number, social security number, or any permutations thereof.

3. Complexity (upper/lower case, numeric, special characters) are not required, but allowed.

4. Passwords must not be based on the City's name or geographic location.

NOTE: Think of your password as a passphrase. Try to create a passphrase that can be easily remembered and easily typed. For example, "baseball-football-track" or "ireallyenjoyvacations". IMPORTANT: Do NOT use these examples as your passphrase!

Password Protection Requirements

1. Passwords should be treated as confidential information. No employee is to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members, under any circumstances.

2. If someone demands your password, refer them to this policy or have them contact the Information Security Officer in IT.

3. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to city resources via the City's IPsec-secured Virtual Private Network or SSL-protected web sites.

4. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in a City approved password manager application.

5. An employee may not circumvent password entry with auto logon (with the exception of a password manager), application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup solutions) with the approval of the Information Security Officer. In order for an exception to be approved there must be a procedure for changing the passwords that adheres to this policy.

6. Passwords used to gain access to city systems should not be used as passwords to access non-City accounts or information (e.g., personal ISP account, personal email account, benefits, etc.).

7. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately.

8. The IT Department or its delegates may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

9. Computers, servers, personal digital assistants, or other computing devices must not be left unattended without enabling a password-protected screensaver or logging off the device.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.