City of Frisco

Information Security Policy

Topic: Information Security Policy **Effective Date: 5/17/2022**

Approved by Ordinance: 2022-05-20 **Revision Date:**

Overview

Information is an essential City of Frisco ("City") asset and is vitally important to the City's business operations. The City must ensure that its information assets are protected in a manner that is cost-effective and that reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

Purpose

To ensure data that the City accesses, stores, transmits, or processes is properly protected from unauthorized disclosure or modification, is retained and/or produced in accordance with the City's Records and Information Management Program, and is available for use.

Scope

This policy applies to all employees, part-time / temporary workers, elected and appointed officials, and contractors / vendors that have been granted access to a City information system, perform work on behalf of the City, and/or maintain City information system data ("Users").

Policy General

This policy is owned by the *Information Technology* (IT) Department and will be reviewed annually to ensure the policy evolves to combat new threats and risks to information assets as well as complies with applicable laws and regulations.

Failure to comply with this policy can result in disciplinary action up to, and including, termination of access and/or employment for employees or access and/or termination of contracts for contractors, partners, consultants, vendors, or other Users. The City may, but is not required to, follow progressive discipline when a violation of this policy occurs. Legal action also may be taken including, but not limited to, action under Texas Penal Code, Computer Crimes, Chapter 33, or other state and federal laws and regulations. The City may also require

restitution for costs associated with system restoration, hardware, or software costs caused by a User in violation of this policy.

Table of Contents

1 What is Information Security

Information Security is a set of controls, processes and methodologies used to protect the confidentiality, integrity, and availability of information assets by implementing physical, administrative, and technical controls.

2 Internal Organization of Information Security

The *Information Security Officer* (ISO) will report directly to the *Chief Information Officer* (CIO) and will be responsible for the overall maintenance, communication interpretation, and enforcement of this policy in coordination with Human Resources (HR) and the City Manager's Office (CMO).

The ISO is responsible for managing and coordinating all security-related activities within the City and is authorized and approved to conduct security assessments, vulnerability scans, network penetration tests, and to work with a variety of security tools required to properly identify and mitigate risk to the City's information assets.

3 Security Framework

The ISO is responsible for managing the implementation of the *NIST Cybersecurity Framework* (NIST) standard that will provide the necessary mechanisms to protect information assets.

For IT employees and others that have responsibility of technology systems, additional information and technical requirements to this policy are detailed in the *Information Security Standard Operating Procedures* (IS-SOP) guide.

4 Reporting Security Incidents

Users should report suspicious cybersecurity incidents directly to their immediate supervisor and Information Technology (IT), by sending an e-mail to IT - Security@friscotexas.gov followed up by submitting a Help Desk ticket. If the incident is of a serious nature that requires immediate response and is after business hours, Users are directed to call the 24-hour hotline at 972-292-5911. If the incident involves a suspicious e-mail, Users should report the e-mail by using the *Phish Alert Button* (PAB) feature in Outlook.

4.1 Incidents Involving Criminal Justice Information Services (CJIS) Information

A substantiated security incident that confirms CJIS information has been disclosed without authorization requires additional reporting requirements as defined in Section 5.3 of the *Criminal Justice Information Services Security Policy.*

5 Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions if it is required for a specific job or law enforcement function, contract, or other use related to City operations, and has been approved in writing by the ISO. Under no circumstances is a User authorized to engage in any activity that is illegal under local, state, federal or international laws or regulations and/or prohibited by City policy or guidelines, while utilizing City resources and/or while acting as a City employee, contractor, or representative. The User in whose name a system account is issued will be responsible at all times for its proper use and/or access. The list below is by no means exhaustive but constitutes an attempt to provide a framework of activities which fall into the category of unacceptable use. Unacceptable use includes, but is not limited to:

- The installation or distribution of "pirated" software products.
- The installation of software that are not appropriately licensed and approved for use by IT.

- Unauthorized copying of copyrighted material including, but not limited to, photographs from magazines, books, the Internet, or other copyrighted sources.
- Intentional introduction of malicious programs into the network, servers, or desktop computers (e.g., viruses, worms, Trojan horses, malware, ransomware, etc.).
- Attempting to harm or harming City equipment, materials, or data.
- Attempting to send or sending anonymous messages of any kind.
- Submitting, publishing, or displaying on the City system, any defamatory, intentionally inaccurate, harassing, abusive, obscene, profane, sexually oriented, or threatening materials or messages, whether public or private.
- Accessing inappropriate web sites to include, but not limited to, pornographic, gambling, or other sites that could be deemed as inappropriate for the workplace.
- Making fraudulent offers of products, items, or services originating from any City account.
- Forging, or attempting to forge, electronic messages and/or other data of another User.
- Intentionally causing a security breach or disruption of the City's system and/or network services. Security breaches include, but are not limited to, accessing data without authorization, exporting data without authorization and providing to a third-party, or providing access to data to others that are not authorized by the City.
- Conducting a Denial-of-Service attempt against the network or a brute-force attack.
- Port scanning, vulnerability scanning, or penetration testing without authorization from the ISO.
- Any form of network monitoring with the intent to intercept data.
- Intentionally circumventing security controls established by the City.
- Circumventing the process of User authentication or authorization to resources.
- Providing information about, or lists of, City employees to parties outside the City, except as required for normal business operations, unless otherwise authorized by the ISO, CMO, or their designee(s) in compliance with applicable state and federal laws and regulations.
- Using City resources for personal gain, financial gain and/or for commercial activity.
- Using a proxy or a *Virtual Private Network* (VPN) not approved by IT.
- Disabling, or attempting to disable, a filtering device on the City's system.
- Sending unsolicited "junk/SPAM/bulk e-mail" or other advertising material to individuals who did not specifically request such material.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes.
- Attempting to access the account, information resources, files or documents of another User without authorization.
- Sharing a User's username/password with another User.
- Sending *Social Security Numbers* (SSN), *PCI* (Payment Card Industry) credit/debit card information, *Personally Identifiable Information* (PII), or *Personal Health Information* (PHI) data via e-mail without encryption.
- Encrypting communications, other than those specified herein, as outlined in City policies, or at the direction of the ISO or designee.

- Using a personal e-mail address to conduct City business. An exception to this is the use of an external e-mail address for testing purposes approved by the ISO and the e-mail does not contain any PII, PCI, PHI, CJIS, or other sensitive City data.
- Users are not authorized to forward City e-mail (messages or attachments) containing PII, PCI, PHI, or CJIS information to a personal e-mail account. The only exception to this is that Users are authorized to forward their own personal data including but not limited to, paystub and tax information, such as W2's, to a personal e-mail address.

6 User Accounts and Passwords

A unique network account will be created for each User. Accounts will be created with the minimum level of access required for an individual to perform a job function (least privilege). User accounts are not authorized to be a member of the Local Administrator group unless approved by the ISO.

Users are responsible for creating unique passwords (*passphrases*) that contain a minimum of 20 characters. Passwords must be changed at a minimum annually, unless it is suspected that the password has been compromised in which case the password should be changed immediately and notification made to IT.

The password policy is available for review via the Policy Page on friscotexas.gov and also as a link via the *Resources Menu* at the top of the FriscoLink home page.

7 Securing Computing Assets

Computers and smart devices must be properly configured to provide the necessary controls to protect the data. While technical controls can be leveraged to secure configurations, the end-User also plays an important role in meeting this objective. Users shall:

- Secure computers, smartphones, and iPads when away by invoking the screen lock or screensaver on the device.
- Physically secure devices to help prevent theft.
- Never open or click on unknown attachments or click on suspicious links as both methods can introduce viruses, malware, or ransomware into the network.
- Never disable the screensaver or screen lock feature.
- Never modify security configuration settings.
- Never bypass authorized logon procedures.
- Never install unauthorized software or hardware.

8 Securing Sensitive Data

Printed material containing sensitive data (PCI, PHI, CJIS, PII) shall be secured by storing the material in a locked area and/or cabinet and not left unsecured.

Sensitive data that is on the City's system, including data displayed on a computer screen, should be secured from unauthorized viewing. Users must be aware and react accordingly when

others might be able to view sensitive data via “shoulder-surfing,” and routinely lock the computer screen when away.

9 Maintenance and Disposal of Digital Media and Printed Material

Users shall maintain all digital media or printed media in accordance with the City’s Records and Information Management Program, Ordinance 2021-06-40. The disposal of digital media or printed material must also comply with the City’s Records and Information Management Program.

Media of all types (digital and printed) shall be destroyed in a manner to render the media, or material, unrecoverable when the data is no longer required.

10 Security Awareness Training

In accordance with Chapter 2054, Subchapter N-1, of the Texas Government Code, all Users are required to complete an annual security awareness training course. The ISO will coordinate with the *Human Resources* (HR) department to deliver the approved training material annually. Failure to comply with this policy can result in disciplinary action up to, and including, termination of access, contracts and/or employment of Users.

10.1 CJIS Training

For all personnel who have access to CJIS data, the continuing security awareness training requirement is biennially. See Section 5.2 in the *Criminal Justice Information Services Security Policy* for additional requirement details.

10.2 CJIS Required Training Topics

CJIS has different levels of security awareness training requirements based upon authorization levels. See Section 5.2.1 and Section 5.3.3 for specific requirements as defined in the *Criminal Justice Information Services Security Policy.*

11 Pre-Employment Checks

The HR department will be responsible for conducting pre-employment background screening procedures on all applicants prior to employment.

If an applicant will have access to CJIS data, additional screening shall be conducted as described in the *Criminal Justice Information Services Security Policy.*

12 Separation from the City

Supervisors should ensure that notification is made immediately to remove all access (network, building, et al.) when User separates from, and/or terminates its contract or relationship with, the City. While the supervisor should work directly with HR to ensure that building access is disabled, a helpdesk ticket should be submitted to IT to request network and application access to be disabled.

If access must be disabled immediately, in addition to submitting a help desk ticket, the supervisor should call the ISO, Enterprise Technology Officer or CIO to ensure the request was received so access can be promptly disabled.

13 Expectation of Privacy

Users, including Temporary Custodians as defined under the Texas Public Information Act (TPIA), shall have no expectation of privacy with respect to the City's telecommunications, networking or information processing systems, including, but not limited to, stored computer files, all work product, e-mail and voice messages, and/or Internet browsing. Any activity and all files or messages on or using any of City systems may be monitored at any time without notice to the User. The City is subject to open records requests and any City-related information or correspondence on any computing device, including cellular phones, may be subject to public disclosure through the TPIA or other law. All Users, including Temporary Custodians, must comply with directives from the City's PIO to ensure compliance with the TPIA and other applicable law.

14 City Property

All Internet/Intranet/Extranet related systems, including, but not limited to, computer equipment, telephone equipment, software, operating systems, storage media, network accounts providing access to e-mail, and web browsing history are the property of the City and, as such, are to be used for purposes related solely to an individual's job with the City, subject to exceptions as noted below. For security and network maintenance purposes, individuals authorized by the ISO may monitor equipment, systems, and network traffic, including, but not limited to, network accounts providing e-mail, at any time. The City reserves the right to audit, inspect and/or search networks and systems on a periodic basis, as approved by the CMO, to ensure compliance with this policy.

15 Glossary

Term	Definition
CJIS	Criminal Justice Information Services – a division of the United States Federal Bureau of Investigation that publishes a security policy mandating the requirements for accessing and protecting certain data elements for law enforcement agencies.
IS-SOP	Information Security Standard Operating Procedure – An additional document that outlines technical requirements.
ISO	Information Security Officer – individual accountable for all aspects of the City's information security program.
NIST	National Institute of Standards and Technology – a federal agency within the Department of Commerce that defines technology standards.
PAB	Phish Alert Button – a feature in Outlook that when used, sends the suspicious e-mail to IT to investigate.
Passphrase	A password that is comprised of more characters, is difficult for attackers to crack or guess, but easier for the User to remember as it is constructed from something that is easy for the User to remember.

PCI	Payment Card Industry – a security standards council that champions for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection to protect credit card data.
PHI	Protected Health Information – demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care.
PII	Personally Identifiable Information – data elements that, when combined, can potentially identify an individual.
PII Data	Data that includes an individual's name with one or more of the below data elements: • Social Security Number • Driver's license or identification number • Financial account numbers or credit/debit card numbers with security access codes or passwords • Medical information • Health insurance information A username or e-mail address in combination with a password or security question and answer which would permit access to an online account
Security Incident	An event that indicates the confidentiality, integrity, or availability of a City information asset may have been compromised.
Shoulder-Surfing	A type of social engineering when someone watches over a User's shoulder to see the information on the screen.
VPN	Virtual Private Network – a method used to encrypt communications between two end-points.

Version	**Release Date**	
1.0	TBD	
		Description