City of Everman Texas
Cyber Security Policy

Adopted: March 10, 2026

I. OVERVIEW

Information is an essential City of Everman ("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.

To that end, this manual furnishes a blueprint for the performance of this City's activities in accordance with established state and national standards. Providing all members of the City with an understanding of the City's mission and its values provides guidance for decision making when situations are not covered by direct policy or procedure.

II. 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.

III. SCOPE

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

IV. POLICY GENERAL

This Policy is will be reviewed annually to ensure the policy evolves to combat new threats and risk 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 5
2 Internal Organization of Information Security 5
3 Security Framework 5
4 Reporting Security Incidents 5
5 Unacceptable Use 5
6 User Accounts and Passwords 6
7 Securing Computing Assets 7
8 Securing Sensitive Data 7
9 Disposal of Digital Media and Printed Material 7
10 Security Awareness Training 7

1. What is Information Security

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

2. Internal Organization of Information Security

The City of Everman shall designate an individual (ISO) responsible for the overall maintenance, communication, interpretation, and enforcement of this policy. This individual will coordinate with Human Resources and the City Manager's Office to manage all security-related activities, including security assessments, vulnerability scans, and risk mitigation for the City's assets.

3. Security Framework

The City will utilize recognized security standards, such as the NIST Cybersecurity Framework, to provide the necessary mechanisms to protect information assets.

4. Reporting Security Incidents

Users must report suspicious cybersecurity incidents immediately to their supervisor and the designated IT authority.

- **Serious Incidents:** If an incident is of a serious nature and occurs after business hours, users should follow established emergency contact protocols.
- **Criminal Justice Information (CJIS):** Any substantiated incident involving the unauthorized disclosure of CJIS information requires additional reporting as defined by federal CJIS Security Policy.

5. Unacceptable Use

Users are prohibited from engaging in illegal activities or actions that violate City policy while utilizing City resources. Unacceptable use includes, but is not limited to:

- Installing "pirated" or unlicensed software.
- 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.). The installation of software that are not appropriately licensed and approved for use by IT.
- Attempting to harm or harming City equipment, materials, or data.
- Accessing inappropriate web sites to include, but not limited to, pornographic, gambling, or other sites that could be deemed as inappropriate for the workplace. Conducting unauthorized port scanning or penetration testing.
- Using City resources for personal or commercial financial gain.
- Sharing account usernames or passwords with others.
- 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.

- 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.
- 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, HR or their designee(s) in compliance with applicable state and federal laws and regulations.
- 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.
- 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 8 characters.
- Passwords must be changed at a minimum annually, 60 days if User is in Police Department, unless it is suspected that the password has been compromised in which case the password should be changed immediately and notification made to IT.

7. Securing Computing Assets

Users play a vital role in securing City hardware and must:

- Secure computers, smartphones, tablets 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

- **Physical Security:** Printed material containing sensitive data (PII, PHI, CJIS) must be stored in locked areas or cabinets.
- **Digital Privacy:** Users must be vigilant against "shoulder-surfing" and ensure sensitive data displayed on screens is secured from unauthorized viewing.

9. Disposal of Digital Media and Printed Material

All media must be maintained and disposed of in accordance with the City's Records and Information Management Program. Media must be destroyed in a manner that renders the data unrecoverable when it is no longer required for City business.

10. Security Awareness Training

In compliance with Texas Government Code Chapter 2054, all Users, including elected and appointed officials who have access to the city's computer systems and use a computer to perform at least 25 percent of their duties, are required to complete an annual security awareness training course supplied by HR. TMLIRP provides training available online free of charge that has been certified by Texas Dept. of Information Resources: https://info.tmlirp.org/cyber-security-training.

,

- **CJIS Training:** Personnel with access to CJIS data must comply to policy supplied in TCRC Policy Manual.

11. GLOSSARY

- 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.
- NIST - National Institute of Standards and Technology – a federal agency within the Department of Commerce that defines technology standards.
- ISO - Information Security Officer – individual accountable for all aspects of the City's information security program. PAB - Phish Alert Button – a feature in Outlook that when used, sends the suspicious email 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.
- ShoulderSurfing - 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.e and arrange for out-of-pocket cash reimbursements, where applicable, using a payment authorization form with the receipts attached.