CO.POL.01 Council Member Electronic Use Policy

Effective Date: 05/11/2021

Purpose

This policy defines how to minimize liability and the risk of damage to data, technology, and information; protect the integrity, availability and confidentiality of technology entrusted to the City of San Marcos (COSM); and protects Council Members from the effects of unauthorized or improper use of technology.

Applicability

Mayor and Council Members during their term on City Council.

Policy Statement

Access

General Access

Access to technology will be granted upon receipt of a written request from the City Clerk's Office. Elected officials are given access to technology through their assigned accounts. Access is controlled and limited only to those systems specifically required to perform job functions. All machines accessing the network must run a supported, up-to-date version of an operating system and anti-virus software.

Unauthorized Access

Council Member may not attempt to gain, or enable another to gain, access to technology for which they have not been approved to use. Council Member may only use their assigned account and are responsible for all activities performed under their account. A Council Member may not share passwords or make their account available to others. A Council Member may not attempt to gain unauthorized access to another user's information. Council Members are not permitted to create local user accounts.

Use

Appropriate Use

Council Member will use technology for the purpose of fulfilling their public services duties and responsibilities. Appropriate use applies to proper care and maintenance of technology as well as following best practice security measures relating to technology use. Limited, occasional or incidental use of the City's technology by Council Members for personal, non-business reasons are acceptable. However, Council Members shall not use City technology to transmit, retrieve, or store any information or communication that is discriminatory, harassing, derogatory to any individual groups, obscene, defamatory or threatening, illegal or otherwise contrary to the City's interest.

Inappropriate Use

Council Member shall not purposefully or negligently cause security breaches which include, but are not limited to: circumventing or attempting to avoid the user authentication or security of any City account; performing any form of unauthorized network monitoring to intercept electronic data not intended for the authorized user; modifying system configurations; introducing unauthorized devices (e.g., rogue access points, hubs, switches, routers, etc., for both hardware and software) into the network to provide unauthorized access to network resources.

Council Member shall not violate copyright laws. This includes the act of pirating software, or the use of pirated software, and the illegal duplication of promulgation of information and other intellectual property that is under copyright. Receipt and use of unauthorized software copies and licenses is prohibited.

Use of City-owned technology or information for personal profit is not permitted.

Council Member shall comply with all applicable local, state, and federal laws and regulations while using City-owned technology.

Password Requirements

Each individual user account requires a password to authenticate the account with City of San Marcos systems. Accounts have applicable categories that determine the length, complexity, and expiration time of their password. User account passwords shall be set by the owner of the user account. User account passwords shall not be shared with any third party. Passwords shall not be printed or written on any physical medium, such as a notepad or notebook. The individual user account password shall not be reused on any other account.

If a password requires a reset, the user account owner shall reset the password using their Multifactor Authentication option using the Self-Service Password Reset (SSPR). If the user account owner cannot reset the password using SSPR, then an in-person reset shall be performed by IT Service Desk. Password resets shall not be provided remotely. If the password has been shared or provided to a third party, a password reset shall occur. If passwords are stored electronically, the file must be encrypted and password protected or saved in an approved password management service. Information Technology shall maintain a Banned Password Dictionary (BPD) containing words or phrases based on their association with local, cultural, or other commonalities of the City of San Marcos and the State of Texas. The content of the BPD shall not be made public. If an attempted password uses a word or phrase in the BPD, it will be rejected.Council user accounts shall have the following characteristics

- Password length of 12 characters at a minimum.
- Requires mixed case letters and numbers or symbols.
- No password expiration.
- Password must not match any words in the Banned Password Dictionary (BPD).
- Must be Multifactor Authentication (MFA) Compliant.

Council Member Responsibilities

Council Member is responsible for:

- password protection,
- proper logout from all open applications,
- proper logout from the virtual machine used to access the council agenda during a Council meeting in the council chambers, and
- ensure all data to be retained is stored on a network or shared drive.

Council Member is responsible for complying with all Council policies and procedures as they apply to technology use, data security, and use of protected health information or other private information, guarding information from unauthorized access or use.

Council Member is responsible for using appropriate security solutions, including but not limited to: securing or locking technology before leaving it unattended and identifying and reporting security-related problems and issues to the Information Technology Department.

Council Member shall have no expectation of privacy with use of any City provided technology. The City is subject to open records requests through the Texas Public Information Act and to the right of Discovery in legal actions brought against the City. Council Member should be aware that all usage may be subject to review or disclosure, without advanced notice, as part of a policy or legal compliance associated with a local, state or federal law and regulation.

Council Member should not store data on the local operating system drive, as this could result in permanent data loss.

Council Member shall notify and coordinate with IT for any hardware, software, upgrades, or modifications of any kind.

Cybersecurity Awareness Training

Council Member shall complete Cybersecurity Awareness Training within 30-days after taking office.

Council Member shall comply with the State of Texas Government Code 2054.5191, requiring all elected officials to complete annual Cybersecurity Awareness Training.

Every April, the City Information Technology Department initiates the annual Cybersecurity Awareness Training campaign. During this time, Council Members will receive instructional emails and access to assigned training. Council Members will have 60 days to complete the training. The city will disable accounts once the deadline has passed and keep them disabled until the training is completed.

Review Process

This policy will be reviewed at a minimum every three years.

Policy Last Review Date – 8/1/2025

Policy Next review Date – 8/1/2028