

RESOLUTION NO. 2021-51R


A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SAN MARCOS, TEXAS APPROVING AN UPDATED COUNCIL TECHNOLOGY ACQUISITION POLICY, COUNCIL ELECTRONICS USE POLICY, AND A COUNCIL POLICY ACKNOWLEDGEMENT FORM THAT PROVIDES GUIDELINES, EXPECTATIONS AND RESPONSIBILITIES FOR THE PROCUREMENT AND USE OF TECHNOLOGY USED BY THE CITY COUNCIL, AND ALIGNS HARDWARE STANDARDS FOR DEVICES USED BY THE CITY COUNCIL WITH THE CITY'S CURRENT STANDARDS; AND DECLARING AN EFFECTIVE DATE.

BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF SAN MARCOS, TEXAS:

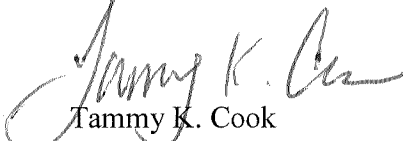
PART 1. The attached Council Technology Acquisition Policy, Council Electronics Use Policy, and Council Policy Acknowledgement Form are hereby approved.

PART 2. This resolution shall become effective immediately from and after its passage.

ADOPTED on May 18, 2021.


Jane Hughson
Mayor

Attest:


Tammy K. Cook
Interim City Clerk

Council Technology Acquisition Policy

1.0

Purpose

This policy defines guidelines, expectations and responsibilities for the procurement and use of technology and aligns a hardware standard for our Mayor and Council Members with the City's current standards

2.0 Applicability

Mayor and Council Members during their term on City Council.

3.0 Policy

Statement

At the request of the Council Member the City will provide an appropriate technological device to facilitate their public service responsibility. Devices will be selected from the Council approved hardware catalog and will follow IT standards for hardware and software specifications. All City purchases will follow local & state purchasing regulations.

Council Member Laptop or Tablet

Council Member will have the choice of requesting a City-owned laptop or they may use their monthly Council compensation stipend for unreimbursed expenses to purchase a Council Member-owned laptop

- For a City-owned laptop or tablet, the City will purchase and provide a device selected from the approved hardware list (See Council approved hardware catalog) that will include: the latest operating system, mobile device management security software, and any additional software needed to fulfill their duties while in office. Remote Access support software will be optional. If software is declined, the Council Member will have to bring the physical device to the IT office for technical support. Council Member's access and use will adhere to the Council Member Electronic Use Policy.
- For a Council Member-owned laptop or tablet purchased through the Council Member's monthly compensation stipend, the City will not purchase or provide licensed software or hardware support. The IT Department will be limited to only installing and assisting with the virtual desktop connection software to allow the Council Member to remotely access the city provided virtual desktop.
- During a Council Member's term, he or she will have the ability to participate in discounted technology programs that are provided to the City. These programs include the purchase of both hardware and software. To find out more about these programs, Council Member's will need to contact the City Clerk's office and request a list of the current programs.

Note: During Council meetings held within the Council Chambers, Council Members are not obligated nor required to bring any additional technology to use during meetings. The City provides each Council Member a desktop computer with access to a virtual desktop to view packets during meetings.

Council Technology Acquisition Policy

Council Cell Phone

Council Members will have the choice of requesting a City-owned cell phone or they may elect to use their personal phone and receive a monthly stipend.

- For a City-owned cell phone, the City will purchase and provide a phone selected from the approved hardware list (See Council Approved Hardware Catalog). The City will be responsible for providing a cell phone, incurring all setup charges, support and providing coverage under the current City's data and voice plan. In the case of a lost/stolen/damaged cell phone, the City is responsible for the replacement cost and terminating of services.
- For a Council Member-owned phone, the City will provide a stipend based on the rate disclosed in the Council Cellular Allowance form. The Council Member must complete, sign and submit the cellular allowance form to the City Clerk's office for processing. The Council Member is responsible for purchasing the equipment, selecting a phone/data plan based on their needs, support and paying all setup and monthly fees associated with the cell phone. In the case of a lost/stolen/damaged cell phone, the Council Member is responsible for the replacement cost.

Multiple Council Terms

- If Council Member is elected to multiple terms, he or she will retain their technology for their new term.
- Technology shall be replaced once it has exceeded the manufacture warranty or it is determined that the technology no longer meets minimum functional requirements for use.

End of Council Term

At the end of the Council Member's term, he or she will have the option of surrendering all technology devices to the City or purchasing and retaining the City-owned technology at a depreciated value as described below.

- For a Council Member to retain their technology, the City will calculate the depreciated value by taking the original purchase price of the technology and depreciate it over seven-years. The Council Member will be responsible for paying the remaining value of the device, including sales tax. The City Information Technology Department will remove all licensed software from the device prior to purchase.

Council Member Electronic Use Policy

1.0 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.

2.0 Applicability

Mayor and Council Members during their term on City Council.

3.0 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.

Council Member Electronic Use Policy

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

All passwords shall conform to the guidelines described below:

Council Member is responsible for the security of their passwords and must not share them. If a Council Member is asked to reveal their password, the requestor should be referred to the Information Technology Department. Council Member should never write passwords down, hint at the format of their password, or use the "Remember Password" feature. It is recommended that Council Member use a unique password for each of their accounts. All passwords shall be changed every 90-days to align with security industry best practices. Users will be notified 14-days in advance prior to password expiration, user will continually be notified each day until password is changed or expired.

Strong passwords have the following characteristics:

The City complies with password complexity standards. A strong password contains more than eight characters and is a passphrase (Ohmy1sturbedmyt0e); is not a word in any language, slang, dialect, jargon, etc.; are not based on personal information. They contain both upper and lower case characters (e.g., a-z, A-Z); have digits and punctuation characters as well as letters (e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:"';<>?,./);

Poor, weak passwords have the following characteristics:

Contains less than eight characters. Personal information such as birthdays, addresses and phone numbers. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. Any of the above spelled backwards. Any of the above preceded or followed by a digit (e.g., secret1, 1secret). The password is a word found in a dictionary. The password is a common usage word such as: names of: family, pets, friends, co-workers, fantasy characters, hardware, software, etc.

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

Council Member Electronic Use Policy

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 HB 3834, 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.

Council Electronic Policy Handbook Acknowledgement Form

I understand and acknowledge the following:

I acknowledge that I have received the following policies and will be accountable to adhere to the information contained within them.

I understand that if I have questions, at any time, regarding any of these policies, I will consult with the City Clerk, or the City Manager.

The policies listed below are included in the City of San Marcos Council Electronic Policy Handbook:

- Council Electronic Policy
- Council Member Electronic Use Policy

These policies will be provided to Council Members by the City Clerk both by hard copy and electronically.

I understand that violation of these policies may result in denial of access to the City's network and could subject me to civil or criminal penalties if I violate local, state or federal laws.

My signature below acknowledges my agreement that I have received and will comply with the above listed policies:

Council Member Signature

Date

Printed Name