Policy: Social Networking/Prohibited Technologies	**Policy No.** 300.17
Chapter: 300.00 Employee Conduct & Welfare	**Effective Date:** 11/12/2024

TO BE COMBINED WITH OUR SOCIAL NETWORKING POLICY NO. 300.17

STATEMENT OF PURPOSE:

Pursuant to Texas S.B. 1893, the City hereby adopts a policy prohibiting the installation or use of TikTok or any application covered by Chapter 620 of the Texas Government Code on any device owned or leased by the City and requiring removal of the application from those devices if already installed. The City shall also adopt a policy prohibiting the employee use of those application for City-related business. TikTok may be installed and used to the extent necessary for providing law enforcement or developing or implementing information security measures, and used in in compliance with documented measures to mitigate risks to the security of governmental entity information. In addition to the State-directed prohibited technologies, City of Mission may add other software and hardware products with security concerns to this policy. Throughout this policy, "Prohibited Technologies" shall refer to the list under Addendum A.

APPLICABILITY:

This policy applies to all City of Mission full and part-time employees, including, paid or unpaid volunteers, and/or any user of the city's network. All City of Mission employees are responsible for complying with the terms and conditions of this policy.

PROCEDURES:

A. CITY-OWNED DEVICES

The download and/or use of prohibited technologies is prohibited on all city-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

The City of Mission shall identify, track, and control city-owned devices to prohibit the installation of or access to all prohibited technologies.

The City of Mission shall restrict access to "app stores" or non-authorized software repositories to prevent the install of unauthorized applications and shall deploy secure baseline configurations, for mobile devices, as determined by City Manager.

The Information Technology Department shall inventory City devices to identify prohibited hardware/equipment manufacturers are in use by the City and report to City Manager with options to transition from these devices.

B. NETWORK RESTRICTIONS
The City of Mission shall configure all firewalls to block access to prohibited technologies, including local networks (LAN), internet access (WAN), virtual private networks (VPN) and on public Wi-Fi operated by the City. This block of network traffic applies to City-owned devices, personal devices of employees and personal devices of the public who use city public Wi-Fi.

COMPLIANCE:

A. All employees shall acknowledge and confirm their understanding of this policy as a part of the City's Personnel Policy Manual review.
B. Compliance with the policy will be verified through various methods, including but not limited to, IT/security system reports and feedback to leadership.
C. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

EXCEPTIONS:

A. Exceptions to the ban on prohibited technologies may only be approved by City Manager.
B. Exceptions to the policy will only be considered when the use of prohibited technologies is required for a specific city business need, such as enabling criminal or civil investigations or for sharing of information to the public during an emergency. To the extent practicable, exception-based use should only be performed on devices that are not used for other city business and on non-city networks.

ADDENDUM A – PROHIBITED TECHNOLOGIES:

The up-to-date list of prohibited technologies is published at http://dir.texas.gov/information-security/prohibited-technologies. The following list is current as of November 12, 2024.

Prohibited Software/Applications/Developers:

- Alipay
- ByteDance Ltd.
- CamScanner
- Kaspersky
- QQ Wallet
- SHAREit
- Tencent Holdings Ltd.
- TikTok

- VMate
- WeChat
- WeChat Pay
- WPS Office
- Any subsidiary or affiliate of an entity listed above.

Prohibited Hardware/Equipment/Manufacturers:

- Dahua Technology Company
- Huawei Technologies Company
- Hangzhou Hikvision Digital Technology Company
- Hytera Communications Corporation
- SZ DJI Technology Company
- ZTE Corporation
- Any subsidiary or affiliate of an entity listed above.