



RESOLUTION NO. 2024-11

A RESOLUTION OF THE CITY OF EAST MOUNTAIN, TEXAS ADOPTING A POLICY PROVIDING PROHIBITING THE INSTALLATION OR USE OF TIKTOK ON CITY DEVICES AND THE USE OF THAT APPLICATION FOR OFFICIAL CITY RELATED BUSINESS PURUANT TO TEXAS SENATE BILL 1893.

WHEREAS, Senate Bill 1893, which went into effect June 14, 2023, Chapter 620 of the Texas Government Code was adopted which requires governmental entities to prohibit the installation or use of TikTok or other designated applications on any device owned or leased by the City and to require removal of the application from those devices if already installed; and,

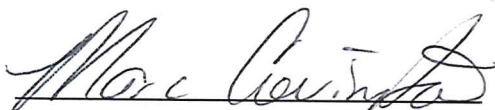
WHEREAS, pursuant to Section 620.004 of the Texas Government Code, TikTok may installed and used to the extent necessary for providing law enforcement or developing or implementing information security measures, and used in compliance with documented measures to mitigate risks to the security of governmental entity information; and,

WHEREAS, the City Commission of the City of East Mountain wishes to adopt the policy required by Chapter 620 of the Texas Government Code to prohibit the use or installation of TikTok on City owned or leased devices and devices used for official City business and to require removal of said application on City owned or leased devices if already installed.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF EAST MOUNTAIN, TEXAS:

1. That the City Council adopts the Prohibited Technologies Security Policy as listed in Exhibit "A."
2. That all city employees shall be provided with a copy of said Policy and acknowledge their receipt of same.
3. That all resolutions or part of resolution in conflict with this Resolution are hereby repealed to the extent of such conflict.
4. That this Resolution shall go into effect immediately upon its adoption by the City Council.

PASSED AND APPROVED this 11th day of November, 2024


Mayor Marc Covington

Attest: 
City Secretary, Lisa Stewart



CITY OF EAST MOUNTAIN

Covered Applications and Prohibited Technology Policy

Date: November 11, 2024

Version: 1.0

CONTENTS

- 1.0 INTRODUCTION 3**
 - 1.1 Purpose..... 3
- 2.0 Covered Applications Policy 3**
 - 2.1 Scope and Definitions 3
 - 2.2 Covered Applications on City-Owned or Leased Devices 3
 - 2.3 Ongoing and Emerging Technology Threats 4
 - 2.4 Bring Your Own Device Policy 4
 - 2.5 Covered Application Exceptions 4
- 3.0 Policy Compliance 5**
- 4.0 Policy Review..... 5**

1.0 INTRODUCTION

1.1 PURPOSE

On December 7, 2022, Governor Greg Abbott required all state agencies to ban the video-sharing application TikTok from all state-owned and state-issued devices and networks over the Chinese Communist Party's ability to use the application for surveilling Texans. Governor Abbott also directed the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) to develop a plan providing state agencies guidance on managing personal devices used to conduct state business. Following the issuance of the Governor's directive, the 88th Texas Legislature passed [Senate Bill 1893](#), which prohibits the use of covered applications on governmental entity devices.

As required by the Governor's directive and Senate Bill 1893, this policy of the City of East Mountain (the "City") prohibits the installation or use of covered applications or prohibited technologies on applicable devices.

2.0 COVERED APPLICATIONS POLICY

2.1 SCOPE AND DEFINITIONS

This policy applies to all City full- and part-time employees, contractors, paid or unpaid interns, and other users of government networks. All City employees are responsible for complying with this policy.

A covered application is:

- The social media service TikTok or any successor application or service developed or provided by ByteDance Limited, or an entity owned by ByteDance Limited.
- A social media application or service specified by proclamation of the governor under Government Code Section 620.005.

2.2 COVERED APPLICATIONS ON CITY-OWNED OR LEASED DEVICES

Except where approved exceptions apply, as described below, the use or installation of covered applications is prohibited on all City-owned or -leased devices, including cell phones, tablets, desktop and laptop computers, and other internet-capable devices.

The City will identify, track, and manage all City-owned or -leased devices including mobile phones, tablets, laptops, desktop computers, or any other internet-capable devices to:

- a. Prohibit the installation of a covered application.
- b. Prohibit the use of a covered application.

- c. Remove a covered application from a City-owned or -leased device that was on the device prior to the passage of S.B. 1893 (88th Leg, R.S.).
- d. Remove an application from a City-owned or -leased device if the Governor issues a proclamation identifying it as a covered application.

The City will manage all City-owned or leased mobile devices by implementing the security measures listed below:

- a. **Restrict access to “app stores” or unauthorized software repositories to prevent the installation of unauthorized applications.**
- b. **Maintain the ability to remotely wipe non-compliant or compromised mobile devices.**
- c. **Maintain the ability to remotely uninstall unauthorized software from mobile devices.**
- d. **Other security measures as may be implemented by the City.**

2.3 ONGOING AND EMERGING TECHNOLOGY THREATS

To provide protection against ongoing and emerging technological threats to the government’s sensitive information and critical infrastructure, DPS and DIR will regularly monitor and evaluate additional social media applications or services that pose a risk to this state.

DIR will annually submit to the Governor a list of social media applications and services identified as posing a risk to Texas. The Governor may proclaim items on this list as covered applications that are subject to this policy.

If the Governor identifies an item on the DIR-posted list described by this section, then the City will remove and prohibit the covered application.

The City may also prohibit social media applications or services in addition to those specified by proclamation of the Governor.

2.4 BRING YOUR OWN DEVICE POLICY

If the City has a “Bring Your Own Device” (BYOD) program, then the City may consider prohibiting the installation or operation of covered applications on employee-owned devices that are used to conduct government business.

2.5 COVERED APPLICATION EXCEPTIONS

The City Manager may permit exceptions authorizing the installation and use of a covered application on government-owned or -leased devices consistent with the authority provided by Government Code Chapter 620.

Government Code Section 620.004 only allows the City to install and use a covered application on an applicable device to the extent necessary for:

- (1) Providing law enforcement; or
- (2) Developing or implementing information security measures.

If the City Council authorizes an exception allowing for the installation and use of a covered application, the City Council must implement measures to mitigate the risks posed to the state during the application's use, to be determined on a case-by-case basis.

The City will document whichever measures it took to mitigate the risks posed during the use of the covered application.

3.0 POLICY COMPLIANCE

All existing employees and all new employees shall sign a document confirming their understanding of this policy.

4.0 POLICY REVIEW

This policy will be reviewed annually and updated as necessary to reflect changes in state law, additions to applications identified under Government Code Section 620.006, updates to the prohibited technology list posted to DIR's website, or to suit the needs of the City.



103 Municipal Dr.
Gilmer, TX 75645
903-297-6041
city.offices2eastmountaintx.gov

Pursuant to Texas S.B. 1893, the City of East Mountain adopted a policy on November 11, 2024, 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 (ie: cell phones, laptops, tablets, desk computers and other devices capable of internet connectivity) and requiring removal of the application from the devices if installed. The policy prohibits the employee use of those applications for city-related business.

The City Council or designee is authorized to execute all documents necessary to complete this transaction.

I, _____ acknowledge that I have reviewed the policy and have removed the prohibited technology from any city owned device and will not re-access the prohibited technology on any city owned device beginning _____, 20__

Employee Signature

Date

Mayor Signature

Date

City Secretary Signature

Date