

ORDINANCE NO. 2024-46

**AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF BURNET, TEXAS, ADOPTING A POLICY PROHIBITING THE USE OF CERTAIN COVERED APPLICATIONS ON CITY-OWNED AND CITY-ISSUED DEVICES AND ON PERSONAL DEVICES USED FOR CITY BUSINESS; PROVIDING FOR EXCEPTIONS AND ENFORCEMENT; AND AMENDING SECTION 2.11 OF THE CITY'S PERSONNEL POLICY**

**WHEREAS**, 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 due to concerns about the application's potential use for surveillance; and

**WHEREAS**, the 88th Texas Legislature subsequently passed Senate Bill 1893, which prohibits the use of covered applications on governmental entity devices; and

**WHEREAS**, the City Council of the City of Burnet recognizes the importance of protecting the City's data, sensitive information, and critical infrastructure from technological threats posed by certain covered applications; and

**WHEREAS**, the City of Burnet is committed to ensuring compliance with state laws and directives concerning the use of covered applications and to taking appropriate measures to safeguard City-owned and City-issued devices.

**NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF BURNET, TEXAS, THAT:**

**Section One. Findings.** The recitals contained in the preamble hereof are hereby found to be true, and such recitals are hereby made a part of this Ordinance for all purposes and are adopted as a part of the judgment and findings of the Council.

**Section Two. Repealer.** All ordinances and codes, or parts thereof, which are in conflict or inconsistent with any provision of this Ordinance are hereby repealed to the extent of such conflict, and the provisions of this Ordinance shall be and remain controlling as to the matters resolved herein.

**Section Three. Adoption of Policy and Amended Personnel Policy.** The Covered Applications and Prohibited Technology Policy is approved and adopted with Exhibit "A" attached to this ordinance, and Section 2.11 of the City's Personnel Policy is hereby amended with Exhibit "B," both in compliance with Senate Bill 1893, which prohibits the use of certain covered applications, including TikTok, on all City-owned and City-issued devices, and on personal devices that are used for City business.

**Section Four. Severability.** If any provision of this Ordinance or the application thereof to any person or circumstance shall be held to be invalid, the remainder of this Ordinance and the application of such provision to other persons and circumstances shall


nevertheless be valid, and the City hereby declares that this Ordinance would have been enacted without such invalid provision.

**Section Five. Open Meetings.** That it is hereby officially found and determined that the meeting at which this ordinance is passed was open to the public as required and that public notice of the time, place, and purpose of said meeting was given as required by the Open Meetings Act, Chapter 551, Loc. Gov't. Code.


**Section Six. Effective Date.** This Ordinance shall be effective upon the date of final adoption hereof.

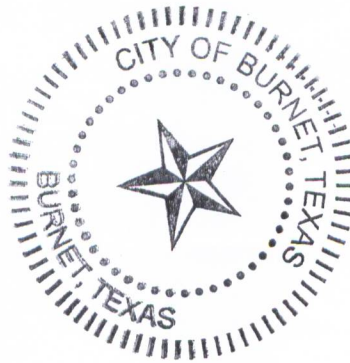
**PASSED, APPROVED, AND ADOPTED** on this 12<sup>th</sup> day of November 2024

**CITY OF BURNET, TEXAS**

  
\_\_\_\_\_  
Gary Wideman, Mayor

**ATTEST:**

  
\_\_\_\_\_  
Maria Gonzales, City Secretary







**Exhibit A**

City of Burnet

Covered Applications and Prohibited  
Technology Policy

Date: November 12, 2024

# CONTENTS

<b>1.0 Introduction</b> .....	<b>3</b>
1.1 Purpose .....	3
1.2 Scope and Application .....	3
<b>2.0 Covered Applications Policy</b> .....	<b>3</b>
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 Personal Device Policy .....	4
2.5 Covered Application Exceptions .....	4
<b>3.0 Policy Compliance</b> .....	<b>5</b>
<b>4.0 Policy Review</b> .....	<b>5</b>

## **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 88<sup>th</sup> Texas Legislature passed Senate Bill 1893, which prohibits the use of covered applications on governmental entity devices.

### **1.2 SCOPE AND APPLICATION**

The City of Burnet's covered applications policy is as described by [Section 2.0](#).

## **2.0 COVERED APPLICATIONS POLICY**

---

### **2.1 SCOPE AND DEFINITIONS**

This policy applies to all City of Burnet full- and part-time employees, contractors, paid or unpaid interns, and other users of City networks. All City of Burnet 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 GOVERNMENT-OWNED OR LEASED DEVICES**

Except where approved exceptions apply, 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.

## **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 PERSONAL DEVICE POLICY**

Employees and contractors may not install or operate prohibited applications or technologies on any personal device that is used to conduct City business, which includes using the device to access any City-owned data, applications, email accounts, VoIP, SMS, video conferencing, and any other City databases or applications.

## **2.5 COVERED APPLICATION EXCEPTIONS**

Upon written request, the city may authorize the installation 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 authorizes an exception allowing for the installation and use of a covered application, the city will use measures to mitigate the risks posed to the state during the application's use.

The city will document whichever measures it takes to mitigate the risks posed to the state during the use of the covered application.

### **3.0 POLICY COMPLIANCE**

---

The city will verify compliance with this policy through various methods, including but not limited to, IT/security system reports and feedback to leadership.

An employee found to have violated this policy may be subject to disciplinary action, including termination of employment.

### **4.0 POLICY REVIEW**

---

This policy will be reviewed periodically 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.

---



## Exhibit B

### Personnel Policy

Note- New text is shown as red and underlined.

#### 2.11 NETWORK AND INTERNET USAGE POLICY AND PROHIBITED TECHNOLOGY APPLICATIONS

The City of Burnet provides Network and Internet Usage for City business when necessary in the performance of the employees' duties. The City is responsible for securing its own network and computing systems in a reasonable and economically feasible degree against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users.

Employees should be aware the City of Burnet's voicemail, e-mail and computer systems are the City of Burnet's property, for the use and benefit of the City of Burnet and that all information stored in these systems is subject to review by management without prior notice to employee and are subject to public inspection under the Texas Public Information Act.

The City Manager will designate a Systems Administrator for all facilities that have access to network or internet usage. To that end, the City has developed the following policy for Network and Internet usage:

- Access – Employee Internet access must be authorized by the System Administrator. A condition of authorization is that all Internet users must agree to this policy as signified by their signature on the acceptance page of this Personnel Policy.
- User password and ID's – Authorized users are assigned a user ID and password upon being given access to the system. User ID's and passwords shall not be changed or altered in any way without express consent of the System Administrator. Protection of the ID and password are the responsibility of the User therefore sharing them with any other person is strictly prohibited. The User can be held responsible for the actions of persons using their ID or password.
- Deletion, examination, copying or modification of files and/or data belonging to other users without their prior consent is prohibited unless specifically authorized by the System Administrator.
- Distribution of information gathered from the system to unauthorized persons is prohibited and the employee is subject to disciplinary action.



- Installation or downloading of hardware or software without the approval of the System Administrator is prohibited and is subject to immediate disciplinary action.
- Employees shall report all computer virus outbreaks to the System Administrator. The System Administrator shall take action reasonably necessary to prevent the spread of a computer virus to other computers.
- Use of facilities for commercial gain is strictly prohibited.
- Use of facilities and/or services for viewing, obtaining, or distributing pornographic materials or other materials not specific to City business is prohibited and will be subject to immediate disciplinary action.
- Any unauthorized, deliberate action, which damages or disrupts any devices on the system including but not limited to viruses or other disruptive/destructive programs, is prohibited and may result in disciplinary action.
- Allowing unauthorized individuals to access system files is prohibited and is subject to disciplinary action.
- Unauthorized use of Electronic Mail is prohibited. This may include sending junk, harassing, obscene or threatening mail; sending solicitations for the purpose of personal financial gain; forgery of electronic signatures; prolonged or excessive use of electronic mail for personal use and/or attempting to read, delete, copy or modify the electronic mail of other users. Any emails of a personal nature should include the following disclaimer "This e-mail contains the thoughts and opinions of the (employee's name) and does not represent official City policy". Personal e-mails are to be kept at a minimum and should not be disruptive to daily activities and responsibilities.
- Violation of copyright laws is prohibited.
- Accessing web sites that charge fees for access, software, services or literature is prohibited unless specifically authorized by the System Administrator, Department Director or Finance Officer.
- Online chat is prohibited.
- Installing and/or playing games is prohibited. Playing online games is prohibited.
- Representing yourself as another person is prohibited.

Some guidelines to avoid unintentional violations are:

- Only access sites on the Internet that are related to your job classification.

- Do not download any files without permission from the System Administrator.
- If by mistake you find yourself in an inappropriate or questionable site, close the browser immediately either by clicking on the small X in the upper right corner or by clicking on File and then close. Notify the System Administrator immediately.
- Never open an attachment that you do not expressly know the contents of. Do not open “junk” email or forward chain letters.
- Make sure your virus protector is enabled at all times. Contact your System Administrator if you are not sure.
- Report any questionable activity or responses to the System Administrator immediately.

### Prohibited Technology Policy

This policy applies to all City of Burnet employees, contractors, interns, and users of City networks.

In response to Governor Greg Abbott's December 7, 2022, directive and Senate Bill 1893, the City of Burnet has implemented this policy to ban the use of TikTok and other covered applications on City-owned devices to protect sensitive information from potential surveillance threats. The Texas Department of Public Safety (DPS), along with the Texas Department of Information Resources (DIR) provide guidance on managing the provisions of this policy.

This policy allows for the identification, tracking, and management of all City-owned or -leased devices.

This policy governs the use of certain applications, particularly:

- TikTok or any successor developed by ByteDance Limited.
- Applications specified by the Governor under Government Code Section 620.005.

Requirements of the policy include:

- Covered applications cannot be installed or used on City-owned or leased devices, including phones, tablets, and computers.
- The City will manage its devices to:
  - Block the installation of covered applications.
  - Remove any prohibited applications.



- Implement security measures, including restricting app store access and remotely wiping non-compliant devices.
- City employees must not install or use TikTok or other prohibited applications on any personal devices that are used for City business, including accessing City data, applications, email, VoIP, SMS, video conferencing, and other City databases.

Written exceptions may be granted for:

- Law enforcement activities.
- Developing or implementing security measures.

The City will monitor compliance using IT/security reports. Violations of this policy may result in disciplinary actions, including termination.

This policy will be updated periodically to align with changes in state law, new applications identified under Government Code Section 620.006, and the City's evolving needs.