**RESOLUTION NO. # 24--007**

**LONE STAR GROUNDWATER CONSERVATION DISTRICT**

**RESOLUTION APPROVING COVERED APPLICATIONS AND PROHIBITED TECHNOLOGY POLICY**

THE STATE OF TEXAS §

COUNTY OF MONTGOMERY §

**WHEREAS**, the Lone Star Groundwater Conservation District ("District") was created by the Legislature of the State of Texas in Acts 2001, 77th Leg., R.S., ch. 1321, p. 3246, § 1(a), as amended;

**WHEREAS**, Senate Bill 1893 (2023) requires the District to prohibit the use of covered applications on District devices;

**WHEREAS**, the Texas Department of Information Resources issued a model policy for prohibiting the use of covered applications pursuant to Senate Bill 1893 on September 16, 2024; and

**WHEREAS,** the Board of Directors of the District determines that adoption of the model policy issued by the Texas Department of Information Resources, with conforming changes relevant to the District, is necessary for compliance with Senate Bill 1893.

**NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF DIRECTORS OF THE LONE STAR GROUNDWATER CONSERVATION DISTRICT AS FOLLOWS:**

1. The above recitals are true and correct and are incorporated herein for all purposes.

2. The Board of Directors of the District hereby approves the District's Covered Applications and Prohibited Technology Policy ("Policy"), attached hereto and incorporated herein for all purposes.

3. The Policy complies with the District's requirements under Senate Bill 1983 (2023).

4. District staff and legal counsel are authorized to take any and all action necessary for the implementation of this Resolution.

AND IT IS SO ORDERED.

PASSED AND ADOPTED this 12th day of November 2024.

**LONE STAR GROUNDWATER CONSERVATION DISTRICT**

By: _____
Jim Spigener, President

ATTEST:

_____
Janice Thigpen, Secretary

# Lone Star GCD

# Covered Applications and Prohibited Technology Policy

Date Adopted: November 12, 2024

# CONTENTS


**1.0 Introduction ..... 3**

1.1 Purpose ..... 3

1.2 Scope and Application ..... 3

**2.0 Covered Applications Policy for Governmental Entities ..... 3**

2.1 Scope and Definitions ..... 3

2.2 Covered Applications on Government-Owned or Leased Devices ..... 4

2.3 Ongoing and Emerging Technology Threats ..... 5

2.4 Bring Your Own Device Policy ..... 5

2.5 Covered Application Exceptions ..... 6

**3.0 Policy Compliance ..... 6**

**4.0 Policy Review ..... 6**

# 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 (2023) 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 model policy establishes a template that entities subject to the directive or bill may mimic to prohibit the installation or use of covered applications or prohibited technologies on applicable devices. The Lone Star Groundwater Conservation District (District) adopts this policy in order to comply with the requirements of Senate Bill 1893 (2023).

## 1.2 Scope and Application

Due to distinctions in requirements between the Governor's directive and SB 1893, the requirements for governmental entities differ somewhat from the requirements for state agencies. This policy is intended to cover the requirements for governmental entities.

Governmental entities, including local governments, must adopt a covered applications policy as described by Section 2.0.

# 2.0 Covered Applications Policy for Governmental Entities

## 2.1 Scope and Definitions

Pursuant to Senate Bill 1893, governmental entities, as defined below, must establish a covered applications policy:

- A department, commission, board, office, or other agency that is in the executive or legislative branch of state government and that was created by the constitution or a

statute, including an institution of higher education as defined by Education Code Section 61.003.

- The supreme court, the court of criminal appeals, a court of appeals, a district court, or the Texas Judicial Council or another agency in the judicial branch of state government.
- A political subdivision of this state, including a municipality, county, or special purpose district.

This policy applies to all District full-and part-time employees, contractors, paid or unpaid interns, and other users of government networks. All District 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 government-owned or -leased devices, including cell phones, tablets, desktop and laptop computers, and other internet-capable devices.

The District will identify, track, and manage all government-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 government-owned or -leased device that was on the device prior to the passage of S.B. 1893 (88th Leg, R.S., 2003).
d. Remove an application from a government-owned or -leased device if the Governor issues a proclamation identifying it as a covered application.

The District will manage all government-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 District will remove and prohibit the covered application.

The District 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 a Governmental Entity is not subject to the Governor's prohibited technology directive but is subject to Senate Bill 1893, it may also consider prohibiting the installation or operation of prohibited technologies and covered applications on employee-owned devices that are used to conduct government business.

If the District has a "Bring Your Own Device" (BYOD) program, then the District may consider prohibiting the installation or operation of covered applications on employee-owned devices that are used to conduct government business. The District may institute a BYOD policy requiring the enrollment of these personal devices in the entity's program before their continued use in conducting governmental business.

## 2.5 Covered Application Exceptions

The District 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 District 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 District authorizes an exception allowing for the installation and use of a covered application, the District must use measures to mitigate the risks posed to the state during the application's use.

The District must document whichever measures it took to mitigate the risks posed to the state during the use of the covered application.

# 3.0 Policy Compliance

The District 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 and updated as necessary every three years, unless the District is required to do so earlier based on legislative changes, 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 District.