



# City of Deer Park

## Covered Applications and Prohibited Technology Policy

Date: November 5, 2024

Version: 1.0

First adoption by Ordinance \_\_\_\_

## CONTENTS

<b>1.0</b>	<b>Introduction</b>	<b>2</b>
1.1	Purpose	2
1.2	Scope and Application	3
<b>2.0</b>	<b>Covered Applications Policy for Governmental Entities</b>	<b>3</b>
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	5
2.6	Network Restrictions	6
<b>3.0</b>	<b>Policy Compliance</b>	<b>6</b>
<b>4.0</b>	<b>Policy Review</b>	<b>7</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.

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.

## 1.2 SCOPE AND APPLICATION

Due to distinctions in requirements between the Governor's directive and SB 1893, Sections 2 and 3 apply to distinct organizations. Where appropriate, each section will identify the unique entities to whom the section applies and the appropriate definitions.

Governmental entities, including local governments, must adopt a covered applications policy as described by [Section 2.0](#).

State agencies to whom the Governor issued his December 7, 2022, directive must adopt a prohibited technology policy as described by [Section 3.0](#). To the extent a state agency is also subject to the requirements of Senate Bill 1893, that agency must also 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 City of Deer Park full and part-time employees, contractors, paid or unpaid interns, and other users of City networks. All City of Deer Park employees utilizing City network resources 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.

City of Deer Park will identify, track, and manage all government-owned or leased devices including cell phones, tablets, desktop and laptop 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.).
- d. Remove an application from a government-owned or leased device if the Governor issues a proclamation identifying it as a covered application.

City of Deer Park 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 City of Deer Park will remove and prohibit the covered application.

City of Deer Park 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 City of Deer Park has a “Bring Your Own Device” (BYOD) program, then the

City of Deer Park 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**

City of Deer Park IT Director 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 City of Deer Park 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 City of Deer Park IT Director authorizes an exception allowing for the installation and use of a covered application, City of Deer Park must use measures to mitigate the risks posed to the city during the application's use including measures that the City of Deer Park IT Director deems appropriate.

City of Deer Park must document whichever measures it took to mitigate the risks posed to the city during the use of the covered application.

## **2.6 NETWORK RESTRICTIONS**

DIR has forbidden access to prohibited technologies on the City's network. To ensure multiple layers of protection, City of Deer Park has also implemented additional network-based restrictions, which include:

- a. Configuring agency firewalls to block access to City's prohibited services on all agency technology infrastructures, including local networks, WAN, and VPN connections.
- b. Prohibiting personal devices from using City technology infrastructure to access prohibited technologies.
- c. With the City of Deer Park IT Director's approval, providing a separate network that allows access to prohibited technologies.

## **3.0 POLICY COMPLIANCE**

---

All City of Deer Park employees utilizing City network resources shall sign a document annually confirming their understanding of the City's covered applications and prohibited technology policies.

City of Deer Park 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, up to and including termination of employment.

## **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 City of Deer Park.