WINTERGARDEN GROUNDWATER CONSERVATION DISTRICT

Covered Applications and Prohibited Technology Policy

Adopted Date: November 13, 2024

CONTENTS

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 document sets for the Wintergarden Groundwater Conservation District's ("District") policy to prohibit the installation or use of covered applications or prohibited technologies on applicable devices.

2.0 Covered Applications Policy for Governmental Entities

2.1 Scope and Definitions

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.).
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 regarding all government-owned or -leased devices to prevent the installation of unauthorized applications on such devices.
b. Maintain the ability to remotely wipe non-compliant or compromised government-owned or -leased devices.
c. Maintain the ability to remotely uninstall unauthorized software from all government-owned or -leased 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 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.

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.

Because those provisions are not applicable to the District's activities, the District will not authorize an exception allowing for the installation and use of a 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 once a year 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 District.