FRISCO ISD

Covered Applications and Prohibited Technology Regulation

Date: November 19, 2024

Version: 1.0

Contents

1.0 Frisco ISD Covered Applications Regulation

1.1 Scope and Definitions

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

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.

1.2 Covered Applications on Frisco ISD-Owned or Leased Devices

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

Frisco ISD will identify, track, and manage all **Frisco ISD**-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 **Frisco ISD**-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 **Frisco ISD**-owned or -leased device if the Governor issues a proclamation identifying it as a covered application.

Frisco ISD will manage all **Frisco ISD**-owned or leased mobile devices by implementing the security measures listed below:

- Restrict access to “app stores” or unauthorized software repositories to prevent the installation of unauthorized applications.
- Maintain the ability to remotely wipe non-compliant or compromised mobile devices.
- Maintain the ability to remotely uninstall unauthorized software from mobile devices.

1.3 Ongoing and Emerging Technology Threats

To provide protection against ongoing and emerging technological threats to sensitive information and critical infrastructure in the State of Texas, the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) will regularly monitor and evaluate additional social media applications or services that pose a risk to the State of Texas.

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 regulation.

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

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

1.4 Bring Your Own Device Policy

Frisco ISD has a "Bring Your Own Device" (BYOD) program, wherein **Frisco ISD** employees may utilize their personal device for some approved **Frisco ISD** business.

Frisco ISD prohibits the operation of covered applications on employee-owned devices while they are being used by the employee to conduct **Frisco ISD** business.

Frisco ISD employees should refrain from installing or operating covered applications on employee-owned devices that are used by the employee to conduct district business.

1.5 Covered Application Exceptions

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

Government Code Section 620.004 only allows **Frisco ISD** 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 **Frisco ISD** authorizes an exception allowing for the installation and use of a covered application, **Frisco ISD** must use measures to mitigate the risks posed to the state during the application's use **including:**

- Access to covered applications is limited to mobile devices:

- used by the **Frisco ISD** Department of Technology for the purposes of developing or implementing information security measures.
- used by the School Resource Officer (SRO) to conduct an official investigation.

2.0 Regulation Compliance

Frisco ISD will verify compliance with this regulation through various methods, including but not limited to, staff training, acceptable use policies and protocols, IT/security system reports and feedback to leadership.

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

3.0 Regulation Review

This regulation will be reviewed 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 **Frisco ISD**