Midland Independent School District

Covered Applications and Prohibited Technology Policy

Date: November 2024
Version: 1.0

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 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 Midland Independent School District full- and part-time employees, contractors, paid or unpaid interns, and other users of government networks. All Midland Independent School 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.
Midland Independent School 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.

Midland Independent School 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 Midland Independent School District will remove and prohibit the covered application.

Midland Independent School District may also prohibit social media applications or services in addition to those specified by proclamation of the Governor.

2.5 Covered Application Exceptions

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

- Limit application use to authorized personnel only.
- Encrypt data transmitted or stored by the application.
- Use a segregated network or VPN for application access.

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

3.0 Prohibited Technology Policy for State Agencies

3.1 Scope

This policy applies to all state agencies to whom the Governor issued his December 7, 2022, directive. This policy applies to all Midland Independent School District employees, including interns and apprentices, contractors, and users of state networks.

All Midland Independent School District employees, contractors, and state network users to whom this policy applies are responsible for complying with these requirements and prohibitions.

3.2 State Agency-Owned Devices

Except where approved exceptions apply, the use or download of prohibited applications or websites is prohibited on all state-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

The Midland Independent School District must identify, track, and control state-owned devices to prohibit the installation of or access to all prohibited applications. This includes the various prohibited applications made available through application stores for mobile, desktop, or other internet capable devices.

The Midland Independent School District must manage all state-owned mobile devices by implementing the security controls listed below:

a. Restrict access to "app stores" or nonauthorized software repositories to prevent the install of unauthorized applications.
b. Maintain the ability to remotely wipe noncompliant or compromised mobile devices.
c. Maintain the ability to remotely uninstall unauthorized software from mobile devices.
d. Deploy secure baseline configurations for mobile devices as determined by Midland Independent School District.

3.3 Personal Devices Used For State Agency Business

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

A state agency that authorizes its employees and contractors to use their personal devices to conduct state business must also establish a "Bring Your Own Device" (BYOD) program. If an employee or contractor has a justifiable need to allow the use of personal devices to conduct state business, the employee or contractor must ensure that their device complies with Midland Independent School District BYOD program, which may include proactive enrollment in the program.

Midland Independent School District BYOD program prohibits an employee or contractor from enabling prohibited technologies on personal devices enrolled in the Midland Independent School District program.

3.4 Sensitive Locations

Midland Independent School District identify, catalogue, and label all sensitive locations. A sensitive location is any location, physical or logical (such as video conferencing, or electronic meeting rooms), that is used to discuss confidential or

sensitive information including information technology configurations, criminal justice information, financial data, personally identifiable data, sensitive personal information, or any data protected by federal or state law.

An employee whose personal device, including their personal cell phone, tablet, or laptop, is not compliant with this prohibited technology policy may not bring their personal device into sensitive locations. This includes using their unauthorized personal to device to access any electronic meeting labeled as a sensitive location.

Visitors granted access to sensitive locations are subject to the same limitations as employees and contractors. If a visitor is granted access to a sensitive location and their personal device has a prohibited application installed on it, then the visitor must leave their unauthorized personal device at an appropriate location that is not identified as sensitive.

3.5 Network Restrictions

DIR has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, Midland Independent School District has also implemented additional network-based restrictions, which include:

a. Configuring agency firewalls to block access to statewide prohibited services on all agency technology infrastructures, including local networks, WAN, and VPN connections.
b. Prohibiting personal devices with prohibited technologies installed from connecting to agency or state technology infrastructure or state data.
c. With the Midland Independent School District executive head's approval, providing a separate network that allows access to prohibited technologies with the approval of the executive head of the agency.

3.6 Prohibited Technologies Exceptions

Only the Midland Independent School District executive may approve exceptions to the ban on prohibited technologies. This authority may not be delegated. All approved exceptions to applications, software, or hardware included on the prohibited technology list must be reported to DIR.

Exceptions to the prohibited technology policy must only be considered when:

- the use of prohibited technologies is required for a specific business need, such as enabling criminal or civil investigations; or
- for sharing of information to the public during an emergency.

For personal devices used for state business, exceptions should be limited to extenuating circumstances and only granted for a predefined period of time. To the extent practicable or possible, exception-based use should only be performed on devices that are not used for other state business and on non-state networks, and the

user should disable cameras and microphones on devices authorized for exception-based use.

3.7 Ongoing and Emerging Technology Threats Pursuant to the Governor's Directive

To provide protection against ongoing and emerging technological threats to the state's sensitive information and critical infrastructure, DPS and DIR will regularly monitor and evaluate additional technologies posing concerns for inclusion in this policy.
DIR posts the list of all prohibited technologies, including applications, software, hardware, or technology providers, to its website. If, after consultation between DIR and DPS, a new technology must be added to this list, DIR will update the prohibited technology list posted on its website.
Midland Independent School District will implement the removal and prohibition of any listed technology on all applicable devices. Midland Independent School District may prohibit other technology threats in addition to those on the posted list should Midland Independent School District determine that such prohibition is appropriate.

4.0 Policy Compliance

All Midland Independent School District employees shall sign a document annually confirming their understanding of the agency's covered applications and prohibited technology policies. Governmental entities that are subject to Senate Bill 1893 but not subject to the Governor's December 07, 2022, directive may elect not to require employees to complete an annual certification.
Midland Independent School District will verify compliance with this policy through various methods, including but not limited to, Technology 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.

5.0 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 Midland Independent School District