Covered Applications and Prohibited Technology Policy

November 5, 2024

Resolution #1449

EXHIBIT A updated 02/07/2024

I. INTRODUCTION

The 88th Texas Legislature passed Senate Bill 1893, which prohibits the use of covered applications and services on devices owned or leased by governmental entities. As required by Senate Bill 1893, the Department of Information Resources (DIR) and the Department of Public Safety (DPS) jointly developed a model policy for governmental entities to use to comply with the law. This policy prohibits the installation or use of covered applications or prohibited technologies on applicable devices.

II. 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 Sulphur Springs employees which are further defined for purposes of this policy as full and part-time employees, City Council members, board appointees, contractors, paid or unpaid interns, and other users of government networks. All City of Sulphur Springs 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.
- Application identified by Department of Information Resources and Department of Public Safety as described under Government Code Section 620.006. The current list of identified covered applications and services will be attached as EXHIBIT A to this policy and is to be updated as needed.

III. COVERED APPLICATIONS ON GOVERNMENT-OWNED OR LEASED DEVICES AND NETWORK

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 Sulphur Springs 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.

City of Sulphur Springs 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.

d. Other measures as needed.

City of Sulphur Springs will prohibit personal devices with prohibited technologies installed from connecting to City technology infrastructure or data.

IV. 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 Sulphur Springs will remove and prohibit the covered application.

City of Sulphur Springs may also prohibit social media applications or services in addition to those specified by proclamation of the Governor.

V. PERSONAL DEVICES USED FOR CITY BUSINESS

Employees may not install or operate prohibited applications or technologies on any personal device that is used to conduct City business, which includes using the device to access any City-

owned data, applications, email accounts, non-public facing communications, City email, VoIP, SMS, video conferencing, and any other City databases or applications.

VI. COVERED APPLICATION EXCEPTIONS

City of Sulphur Springs 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 Sulphur Springs 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.

For any authorized exception, the City of Sulphur Springs must use measures to mitigate the risks posed to the City during the application's use including:

- Disabling cameras and microphones while covered application is in use
- Logging out of application after exception-based use is completed
- Requiring device to be password protected to access it.

City of Sulphur Springs must document whichever measures it took to mitigate the risks posed to the City during the use of the covered application.

Only the City Manager may approve exceptions to the ban on prohibited technologies. This authority may not be delegated to department heads or any other position. When using covered applications for purposes of law enforcement, a list of devices authorized for exceptions must be approved by City Manager. All approved exceptions to applications, software, or hardware included on the prohibited technology list must then be reported to the City's managed service provider that is either contracted with or employed by the City.

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 city 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 city business and on non-city networks, and the user should disable cameras and microphones on devices authorized for exception-based use.

VII. SENSITIVE LOCATIONS

A sensitive location is a location whether physical or virtual, that is being used to discuss confidential or sensitive information technology configurations, criminal justice information,

employee's sensitive personal information, or items which fall under Government Code Section 551.071 – 551.091, or any other information which protected by state or federal law. An employee or visitor whose personal device is not compliant with this policy may not bring their personal device into sensitive locations.

VIII. POLICY COMPLIANCE

All City of Sulphur Springs employees shall sign a document at the policy's initial adoption or at time of employment, confirming their understanding of the city's covered applications and prohibited technology policies. City of Sulphur Springs will verify compliance with this policy through various methods, including but not limited to, IT/security system reports and feedback to leadership.

This policy shall be distributed to all software providers that the City of Sulphur Springs contracts with or subscribes to. It is the responsibility of the department head using the software to distribute the policy biennially.

An employee found to have violated any part of this policy may be subject to disciplinary action, including termination of employment. An employee violates this policy if an employee that has been granted an exception by the City Manager is found to be using the covered application for personal and social use.

IX. POLICY REVIEW

This policy will be reviewed biennially 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 Sulphur Springs.

EXHIBIT A

This list is to be updated periodically as changes are made on the Department of Information Resources website.

https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies

Prohibited Software/Applications/Developers (as of 1/23/23)

- Alipay
- ByteDance Ltd.
- CamScanner
- DeepSeek (added 1/31/2025)
- Kaspersky
- Lemon8 (added 1/31/2025)
- Moomoo (added 1/31/2025)
- QQ Wallet
- RedNote (added 1/31/2025)
- SHAREit
- Tencent Holdings Ltd.
- Tiger Brokers (added 1/31/2025)
- TikTok
- VMate
- WeBull (added 1/31/2025)
- WeChat
- WeChat Pay
- WPS Office
- Any subsidiary or affiliate of an entity listed above.

Prohibited Hardware/Equipment/Manufacturers (as of 1/23/23)

- Dahua Technology Company
- Huawei Technologies Company
- Hangzhou Hikvision Digital Technology Company
- Hytera Communications Corporation
- SZ DJI Technology Company
- ZTE Corporation
- Any subsidiary or affiliate of an entity listed above.