CITY OF LAGO VISTA

RESOLUTION NO. 24-2081

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF LAGO VISTA, TEXAS ADOPTING A PROHIBITED TECHNOLOGY POLICY AND PROVIDING AN EFFECTIVE DATE.

WHEREAS, the City of Lago Vista, Texas, is a Home Rule City, chartered in 1984, and located in Travis County; and

WHEREAS, Texas Senate Bill (SB) 1893 requires governmental bodies to prohibit the use of certain technology applications to protect cybersecurity and sensitive information; and

WHEREAS, the City Council of the City of Lago Vista desires to adopt a formal policy to comply with this legislative mandate and enhance cybersecurity protections for all City- owned or leased devices.

NOW THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF LAGO VISTA, TEXAS:

SECTION 1. The City Council hereby finds that the recitals set forth above are true and correct and are incorporated into this Resolution as if written herein.

SECTION 2. The City Council of the City of Lago Vista hereby adopts the Prohibited Technology Policy attached hereto as Exhibit A and made a part of this Resolution for all purposes.

SECTION 3. The City Manager or their designee is authorized to implement and enforce the policy as described in Exhibit A, ensuring compliance with Texas Senate Bill (SB) 1893 and protecting sensitive information on all City-owned or leased devices.

SECTION 4. This Resolution shall take effect and be in full force from and after its adoption, and all resolutions of the City Council of the City of Lago Vista in conflict herewith are hereby repealed to the extent of such conflict.

PASSED AND APPROVED THIS THE 7th DAY OF NOVEMBER 2024.

CITY OF LAGO VISTA • TEXAS

APPROVED:

Kevin Sullivan, Mayor

ATTEST:

Susie Quinn, Interim City Secretary

On a motion by Councilor Prince, seconded by ~~Councilor~~ Mayor Pro Tem Marion, the above and foregoing instrument was passed and approved

CITY OF
LAGO VISTA
TEXAS

Prohibited Technology Policy

1.0 Purpose

1.1 Pursuant to Texas Government Code chapter 620, which became effective in 2024, all state agencies, political subdivisions, judicial courts, counties, municipalities and Texas governmental entities are required to ban the video-sharing application TikTok (or any successor application or service developed by ByteDance Limited or an entity owned by ByteDance Limited, or a social media application or service specified by proclamation by the governor) from all government-owned and government-issued devices and networks. The Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) developed a guide for governmental entities on managing personal devices used to conduct governmental business.

1.2 This policy outlines the prohibitions regarding the installation or use of covered applications or prohibited technologies on applicable City devices.

2.0 Scope

2.1 Pursuant to Texas Government Code chapter 620, governmental entities such as City of Lago Vista ("City") must establish a covered applications policy.

2.2 This policy applies to all City full- and part-time employees, interns, officials and other users of the City's networks. All City employees are responsible for complying with this policy.

2.3 A covered application is:

2.3.1 The social media service TikTok or any successor application or service developed or provided by ByteDance Limited, or an entity owned by ByteDance Limited.

2.3.2 A social media application or service specified by proclamation of the governor under Government Code Section 620.005.

3.0 Covered Applications on City-Owned or Leased Devices

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

3.2 City will identify, track, and manage all City-owned or -leased devices including mobile phones, tablets, laptops, desktop computers, or any other internet-capable devices to:

3.2.1 Prohibit the installation of a covered application.

3.2.2 Prohibit the use of a covered application.

3.2.3 Remove a covered application from a City-owned or -leased device that was on the device prior to the passage of S.B. 1893 (88th Leg, R.S.).

3.2.4 Remove an application from a City-owned or -leased device if the Governor issues a proclamation identifying it as a covered application.

3.3 City will manage all City-owned or leased mobile devices by implementing the security measures listed below:

3.3.1 Restrict access to "app stores" or unauthorized software repositories to prevent the installation of unauthorized applications.

3.3.2 Maintain the ability to remotely wipe non-compliant or compromised mobile devices.

3.3.3 Maintain the ability to remotely uninstall unauthorized software from mobile devices.

4.0 Bring Your Own Device

4.1 City prohibits the installation or operation of covered applications on employee-owned devices that are used to conduct government business and are partially or fully funded by the City.

5.0 Additional Prohibited Applications

5.1 To ensure the security and integrity of City-issued devices, installation is prohibited of the following applications:

- TikTok
- Kaspersky
- ByteDance Ltd.
- Tencent Holdings Ltd.
- Alipay
- CamScanner
- QQ Wallet

Date: 11/07/24

- SHAREit
- VMate
- WeChat
- WeChat Pay
- WPS Office
- Any subsidiary or affiliate of an entity listed above.

5.2 Additionally, below is a list of prohibited Hardware/Equipment/Manufactures as of 1/23/2023:

- 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.

These applications pose potential risks related to data privacy, unauthorized access, and the exposure of sensitive corporate information. The prohibited applications list may be expanded from time to time without update to this policy, but with notification to all City network users.

6.0 Ongoing & Emerging Technology Threats

6.1 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 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 will remove and prohibit the covered application.

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

7.0 Policy Compliance

7.1 City will verify compliance with this policy through various methods, including but not limited to, IT/security system reports and feedback to leadership.

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

Date: 11/07/24

8.0 Policy Review

8.1 This policy will be reviewed annually and updated as necessary to reflect changes in state law, additions to applications identified under Texas Government Code chapter 620, updates to the prohibited technology list posted to DIR's website, or to suit the needs of the City.

9.0 References

9.1 Texas Government Code chapter 620.

9.2 Texas Department of Information Resources Guidance.

9.3 The up-to-date list of prohibited technologies is published at https://dir.texas.gov/information-security/prohibited-technology.