

Ordinance No. 2024-25
Village of Salado
County of Bell
November 21, 2024

ORDINANCE NO. 2024-25

AN ORDINANCE OF THE VILLAGE OF SALADO, TEXAS, TO ESTABLISH A COVERED APPLICATIONS AND PROHIBITED TECHNOLOGY POLICY; AND INCLUDING THE FOLLOWING: FINDINGS OF FACT; EFFECTIVE DATE; REPEALER; SEVERABILITY CLAUSE; AND PROPER NOTICE AND MEETING.

WHEREAS, pursuant to Texas Local Government Code § 51.032, the Board of Aldermen (the “Board”) of the Village of Salado, Texas (the “Village”) is authorized by law to adopt an ordinance, not inconsistent with state law, that it considers proper for the government of the Village; and

WHEREAS, The Legislature adopted SB 1893, which requires local governments, including cities, to adopt a policy regarding the use of Tik Tok and other applications on Village-owned and leased electronic devices; and

WHEREAS, the State Department of Information Resources has issued a draft policy for cities to consider that incorporates the requirements of SB 1893; and

WHEREAS, it is deemed in the best interest of the Village for the health, safety, and welfare of its citizens, and to comply with state law, that an ordinance be established to adopt a Covered Applications and Prohibited Technology Policy.

NOW, THEREFORE, BE IT ORDAINED BY THE BOARD OF ALDERMEN OF THE VILLAGE OF SALADO, TEXAS:

SECTION I. ENACTMENT PROVISIONS

- A. Findings of Fact:** All of the above premises are hereby found to be true and correct legislative and factual findings of the Village of Salado and are hereby approved and incorporated into the body of this ordinance as if copied in their entirety.
- B. Popular Name:** This Ordinance shall be commonly referred to as “The Covered Applications and Prohibited Technology Ordinance.”
- C. Scope:** This Ordinance, and the rules and regulations adopted herein, shall apply generally within the Village limits.

D. Effective Date: This Ordinance shall take effect immediately upon passage and publication.

SECTION II. ADOPTION

Ordinance No. 2024-25 is hereby adopted as follows:

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.

The Village of Salado, Texas (the "Village") therefore adopts a policy, based on the model policy proposed by the Texas Department of Information Resources ("DIR"), to prohibit the installation or use of covered applications or prohibited technologies on applicable devices, as required by Senate Bill 1893.

2. Covered Applications Policy for Governmental Entities

A. Scope and Definitions

Pursuant to Senate Bill 1893, a political subdivision of the State of Texas, including a e, must adopt a covered applications policy.

This policy applies to all Village full- and part-time employees, contractors, paid or unpaid interns, and other users of government networks. All Village 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.

3. 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 Village 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 Village will manage all government-owned or leased mobile devices by implementing the security measures listed below:

- a. Prohibit access to “app stores” or unauthorized software repositories to prevent the installation of unauthorized applications on Village owned or leased devices
- b. Maintain the ability to wipe or remove a covered application from any Village -owned or leased device.
- c. To the extent practicable, maintain the ability to remotely uninstall unauthorized software from mobile devices.

4. 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 Village will remove and prohibit the covered application.

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

5. Bring Your Own Device Policy

If the Village has a “Bring Your Own Device” (BYOD) program, then the Village may prohibit the installation or operation of covered applications on employee-owned devices that are used to conduct government business.

6. Covered Application Exceptions

The Village 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 Village 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 the Village authorizes an exception allowing for the installation and use of a covered application, the Village will use measures to mitigate the risks posed to the state during the application's use, including:

- Oversight by the Village Administrator and relevant department head to ensure that use of the covered application is necessary for the performance of the governmental functions allowed in Section 620.004.

The Village will document whichever measures it took to mitigate the risks posed to the state during the use of the covered application.

7. Prohibited Technology Policy

A. Scope

This policy applies to all Village employees, including interns and apprentices, contractors, and users of state networks. All Village employees, contractors, and state network users to whom this policy applies are responsible for complying with these requirements and prohibitions.

B. Village-Owned Devices

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

The Village must identify, track, and control City-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 Village must manage all Village -owned mobile devices by implementing the security controls listed below:

- a. Restrict access to "app stores" or nonauthorized software repositories to prevent the installation 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 the Village.

8. Personal Devices Used For Official 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.

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 the Village's BYOD program, which may include proactive enrollment in the program.

The Village's BYOD program prohibits an employee or contractor from enabling prohibited technologies on personal devices enrolled in the City's program.

9. Sensitive Locations

The Village may 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 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.

10. Network Restrictions

DIR has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, The Village will also implement 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 Village Administrator's approval, providing a separate network that allows access to prohibited technologies with the approval of the Village Administrator.

11. Prohibited Technologies Exceptions

Only the Village Administrator or relevant department head 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 Village 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 Village business and on non- Village networks, and the user should disable cameras and microphones on devices authorized for exception-based use.

12. 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.

The Village will implement the removal and prohibition of any listed technology on all applicable devices. The Village may prohibit other technology threats in addition to those on the posted list should the Village determine that such prohibition is appropriate.

13 Policy Compliance

The Village 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.

14. 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 the Village.

15. RESERVATION OF RIGHTS

All rights and remedies of the Village of Salado, Texas are expressly saved as to any and all violations of the provisions of any other ordinance affecting the streets and roadways of the Village which existed at the time of the effective date of this Ordinance; and as to such accrued violations and all pending litigation, both civil and criminal, whether pending in court or not, under such ordinances, the same shall not be affected by this Ordinance but may be prosecuted until final disposition by the courts.

16. SAVINGS CLAUSE

The repeal of any ordinance or part of ordinances effectuated by the enactment of this ordinance shall not be construed as abandoning any action now pending under or by virtue of such ordinance or as discontinuing, abating, modifying or altering any penalty accruing or to accrue, or as affecting any rights of the Village under any section or provisions of any ordinances at the time of passage of this ordinance.

17. SEVERABILITY CLAUSE

If any provision, section, sentence, clause or phrase of this Ordinance, or the application of the same to any person or set of circumstances is for any reason held to be unconstitutional, void, invalid, or unenforceable, the validity of the remaining portions of this Ordinance or its application to other persons or sets of circumstances shall not be affected thereby, it being the intent of the Board of Alderman of the Village of Salado in adopting, and of the Mayor in approving this Ordinance, that no portion thereof or provision or regulation contained herein shall be come inoperative or fail by reason of any unconstitutionality or invalidity of any portion, provision or regulation.

18. REPEALER CLAUSE

The provisions of this ordinance shall be cumulative of all other ordinances or parts of ordinances governing or regulating the same subject matter as that covered herein, provided, however, that all prior ordinances or parts of ordinances inconsistent or in conflict with any of the provisions of this ordinance are hereby expressly repealed to the extent that such inconsistency is apparent. This Ordinance shall not be construed to require or allow any act which is prohibited by any other Ordinance.

19. EFFECTIVE DATE

This Ordinance shall take effect immediately from and after its passage and publication as may be required by governing law.


20. NOTICE AND MEETING CLAUSE

It is hereby officially found and determined that the meeting at which this Ordinance was passed was open to the public and that public notice of the time, place, and purpose of said meeting was given as required by the Texas Open Meetings Act, Chapter 551 of the Texas Government Code.

21. PUBLICATION

This Ordinance shall become effective immediately upon the date of its publication as required by § 52.011 of the Texas Local Government Code. The Village Secretary is hereby directed to cause the caption of this Ordinance to be published in the manner required by law.

PASSED AND APPROVED on SECOND READING this, the 21st day of November, 2024, by a vote of 4 (ayes) to 0 (nays) and 0 abstentions vote of the Board of Aldermen of the Village of Salado, Texas.


Bert Henry, Mayor

ATTEST:


Debbie Bean, Village Secretary

Approved to Form:

Joshua Katz, City Attorney