



Technology Department

19200 Cobb Avenue

Tornillo, TX 79853

Phone 915.765.3035

Fax 915.765.3099

MEMORANDUM

To:

From:

Subject:

Date:

HISTORY:

RATIONALE:

BUDGET IMPACT:

ADMINISTRATIVE RECOMMENDATION:

Vision: Believe we can succeed, with pride we will achieve.

Mission: The mission of the District is to educate and inspire students in a safe and supportive environment which will result in closing the achievement gap by preparing all students for college readiness and success in a global society.

ARTICLE

Policy Alert: Applications on District-Owned Electronic Devices

Wednesday, November 6, 2024



☆ Save to Favorites



The 88th Legislature passed Senate Bill 1893 prohibiting the use of certain social media applications and services on governmental entity electronic devices. SB 1893 created Government Code Chapter 620, which requires governmental entities to ban “covered applications,” including the social media service TikTok and any applications or services developed or provided by the company ByteDance Limited. The bill also directed the Texas Department of Information Resources (DIR) and the Texas Department of Public Safety to develop a model policy for the prohibition of covered applications.

Governmental entities, as defined by Government Code Chapter 620, have until November 20, 2024, to adopt their own “policy” relating to covered applications. DIR recently published the Model Covered Applications and Prohibited Technology Policy, which can be found on the [DIR website](#).

TASB Policy Service recommends developing an administrative regulation in compliance with SB 1893 before the November 20, 2024, deadline. The DIR model policy can be treated like an administrative regulation and does not require board approval.

Policy CQC(LEGAL) already includes provisions relating to these types of applications on district-owned devices. However, if your district wishes to address this matter in local policy, your policy consultant can provide sample language that can be adopted by your school board.

Need help?

If you have any questions or would like sample local policy language, please contact your [policy consultant](#) at 800-580-7529.

Was this article helpful?

 

- [Policy & Governance](#)
- [Team of Eight](#)
- [Policy Alert](#)
- [Policy Update](#)
- [Technology](#)

Policy Service

TASB Policy Service provides timely, expert, and cost-effective development and updating of board policy and administrative regulations.





Model Security Plan for Prohibited Technologies

Date: Jan 26, 2023

Version: 1.0

TABLE OF CONTENTS

Table of Contents	2
Introduction	3
Background:.....	3
Scope:.....	3
Objectives	3
State AGENCY Security Plan	4
Objective 1: PROHIBIT the download and use of Prohibited technologies on any state-issued device.	4
Objective 2: PROHIBIT employees and contractors from conducting state business on PROHIBITED TECHNOLOGY-enabled personal devices.....	5
Objective 3: Identify sensitive locations, meetings, and personnel within an agency that could be exposed to Prohibited technology-enabled personal devices.....	5
Objective 4: Implement network-based restrictions to prevent the use of prohibited technologies on agency networks by any prohibited technology-enabled Personal device.	6
Objective 5: Coordinate the incorporation of any additional technology that poses a threat to the State’s sensitive information and critical infrastructure into this plan.	7
Exceptions	7
Plan Compliance	8
Addendum A	9

INTRODUCTION

BACKGROUND:

On December 7, 2022, Governor Greg Abbott required (https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_1.pdf) 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 they use to conduct state business.

SCOPE:

This plan applies to all state agencies and institutions of higher education (IHEs), including their employees, contractors, interns, or any users of state-owned networks. Each agency is responsible for the implementation of the plan as outlined in this document, including any changes to meet specific agency needs.

OBJECTIVES

To protect the State's sensitive information and critical infrastructure from technology that poses a threat to the State of Texas, this plan outlines the following objectives for each agency:

1. Ban and prevent the download or use of prohibited technologies on any state-issued device. This includes all state-issued cell phones, laptops, tablets, desktop computers, and other devices of capable of internet connectivity. Each agency's IT department must strictly enforce this ban.
2. Prohibit employees or contractors from conducting state business on prohibited technology-enabled personal devices.
3. Identify sensitive locations, meetings, or personnel within an agency that could be exposed to prohibited technology-enabled personal devices. Prohibited technology-enabled personal devices must be prohibited from entering or being used in these sensitive areas.

4. Implement network-based restrictions to prevent the use of prohibited technologies on agency networks by any device.
5. Coordinate the incorporation of other technology providers as necessary, including any apps, services, hardware, or software that pose a threat to the State's sensitive information and critical infrastructure into this plan.

STATE AGENCY SECURITY PLAN

OBJECTIVE 1: PROHIBIT THE DOWNLOAD AND USE OF PROHIBITED TECHNOLOGIES ON ANY STATE-ISSUED DEVICE.

Prohibited technologies shall not be downloaded or used on any state-issued device. This includes all state-issued cell phones, laptops, tablets, desktop computers, or any other devices of capable of internet connectivity. Each agency must strictly enforce this objective.

To achieve this security plan objective, agencies must implement the following:

1. Agencies must identify, track, and control state-owned devices to prohibit the installation of or access to all prohibited technologies. This includes the various applications for mobile, desktop, or other internet capable devices.
2. Determine if prohibited technologies have been downloaded on state-issued devices. If so, the agency must remove the application from those devices immediately unless an exception has been granted in writing by the agency head and reported to DIR.
3. Configure agency network firewall(s) to block prohibited domains on both the local network and virtual private network (VPN).
4. Manage all state-issued mobile devices by implementing the security controls listed below:
 - a. Restrict access to "app stores" or non-authorized 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 un-authorized software from mobile devices.

- d. Deploy secure baseline configurations, for mobile devices, as determined by the agency.

OBJECTIVE 2: PROHIBIT EMPLOYEES AND CONTRACTORS FROM CONDUCTING STATE BUSINESS ON PROHIBITED TECHNOLOGY-ENABLED PERSONAL DEVICES.

In addition to preventing the use of prohibited technologies on state-issued devices, agencies must prohibit employees and contractors from using prohibited technology-enabled personal devices to conduct state business. State business includes accessing any state-owned data, applications, email accounts, or non-public facing communications. Examples of state network resources include state email, VoIP, SMS, video conferencing, CAPPs, Texas.gov, and any other state databases or applications.

If an agency has a justifiable need to allow the use of personal devices to conduct state business, the agency may establish a "Bring Your Own Device" (BYOD) program with the following considerations:

- a. Ability to manage lost, stolen, or unauthorized devices;
- b. Prevent the installation of banned or unauthorized software;
- c. Prevent the use of unsecure public networks;
- d. Manage open records, confidentiality, and privacy-related issues;
- e. Ability to create a guest security profile that prevents prohibited technologies from communicating or being downloaded while that security profile is in use; and
- f. Ability to remove all state-related business and applications from the personal device before removing the security profile or un-enrolling the device from the BYOD program.

OBJECTIVE 3: IDENTIFY SENSITIVE LOCATIONS, MEETINGS, AND PERSONNEL WITHIN AN AGENCY THAT COULD BE EXPOSED TO PROHIBITED TECHNOLOGY-ENABLED PERSONAL DEVICES.

1. Agencies must identify, catalog, and label sensitive locations within the agency. 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.

2. Agencies must indicate when someone is entering a sensitive location. Physical locations should have exterior signage, and electronic meetings should be labeled.
3. Unauthorized devices, such as personal cell phones, tablets, or laptops, may not enter sensitive locations. This includes any electronic meeting labeled as a sensitive location. Locked storage areas that prevent external communications with the devices stored within may be placed outside of sensitive locations to temporarily hold unauthorized devices when entering a sensitive location.
4. Visitors granted access to secure locations are subject to the same limitations as contractors and employees on unauthorized personal devices when entering secure locations. Agencies are responsible for securing sensitive areas.

OBJECTIVE 4: IMPLEMENT NETWORK-BASED RESTRICTIONS TO PREVENT THE USE OF PROHIBITED TECHNOLOGIES ON AGENCY NETWORKS BY ANY PROHIBITED TECHNOLOGY-ENABLED PERSONAL DEVICE.

DIR Cyber Operations has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, agencies must also implement additional network-based restrictions to prevent communication with prohibited internet services:

1. Agencies must configure firewalls to block access to statewide prohibited services on all agency technology infrastructures, including local networks, WAN, and VPN connections.
2. Agencies must prohibit personal devices with prohibited technologies installed from connecting or attempting to connect to agency or state technology infrastructure or state data.
3. Agencies may provide access to prohibited technologies through a separate network, with the approval of the agency head.

OBJECTIVE 5: COORDINATE THE INCORPORATION OF ANY ADDITIONAL TECHNOLOGY THAT POSES A THREAT TO THE STATE'S SENSITIVE INFORMATION AND CRITICAL INFRASTRUCTURE INTO THIS PLAN.

To provide protection against ongoing and emerging technology threats to the state's sensitive information and critical infrastructure, technologies will be regularly monitored and evaluated for inclusion into this plan.

1. DPS and DIR will evaluate and monitor technologies that pose a threat to state sensitive information and critical infrastructure. They will provide recommendations to state leaders on technologies that should be blocked or prohibited statewide.
2. DIR will host a site (<https://dir.texas.gov/information-security/prohibited-technologies>) that lists all technologies including apps, software, hardware, or technology providers that are prohibited. New technologies will be added to the list after consultation between DIR and DPS.
3. DIR will notify agencies in the event the list is amended.
4. It is the responsibility of each agency to implement the removal and prohibition of any offending technology.
5. The prohibited technologies list current as of January 23, 2023, can be found in Addendum A.

EXCEPTIONS

Exceptions may only be approved by the head of the agency to enable law-enforcement investigations or other legitimate business uses. This authority may not be delegated. All approved exceptions to allow the use of a prohibited technology must be reported to DIR.

Devices granted an exception should only be used for the specific use case in which the exception was granted and only used on non-state or specifically designated separate networks. If possible, cameras and microphones should be disabled on those devices when not in active use for their intended purpose.

For personal devices used for state business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period of time.

IHEs may include an exception to accommodate student use of a state email address provided by the university in the policy submitted to DPS. Any such exception shall be restricted to student's use of a personal device that is privately owned or leased by the student or a member of the student's immediate family, and shall include network security considerations to protect the IHE network and data from traffic related to prohibited technologies.

PLAN COMPLIANCE

Each agency is required to develop its own security policy to support the implementation of this plan. This policy must be submitted by February 15, 2023 to the Department of Public Safety by uploading the document to the SPECTRIM portal. The SPECTRIM portal will be configured to receive these policies by February 1, 2023.

ADDENDUM A

The up-to-date list of prohibited technologies is published at <https://dir.texas.gov/information-security/prohibited-technologies>. The following list is current as of January 23, 2023.

Prohibited Software/Applications/Developers

- TikTok
- Kaspersky
- ByteDance Ltd.
- Tencent Holdings Ltd.
- Alipay
- CamScanner
- QQ Wallet
- SHAREit
- VMate
- WeChat
- WeChat Pay
- WPS Office
- Any subsidiary or affiliate of an entity listed above.

Prohibited Hardware/Equipment/Manufacturers

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



Tornillo ISD

Covered Applications and Prohibited Technology Policy

Date: November 7, 2024

Version: 1.0

CONTENTS

1.0	Introduction	3
1.1	Purpose	3
1.2	Scope and Application	3
2.0	Covered Applications Policy for Governmental Entities	4
2.1	Scope and Definitions.....	4
2.2	Covered Applications on Government-Owned or Leased Devices.....	5
2.3	Ongoing and Emerging Technology Threats.....	6
2.4	Bring Your Own Device Policy	6
2.5	Covered Application Exceptions.....	7
3.0	Prohibited Technology Policy for State Agencies	8
3.1	Scope.....	8
3.2	State Agency-Owned Devices	8
3.3	Personal Devices Used For State Agency Business	9
3.4	Sensitive Locations.....	9
3.5	Network Restrictions.....	10
3.6	Prohibited Technologies Exceptions.....	10
3.7	Bring Your Own Device Policy for a Governmental Entity Not Subject to the Governor’s Prohibited Technology Directive	11
3.8	Ongoing and Emerging Technology Threats Pursuant to the Governor’s Directive	11
4.0	Policy Compliance	12
5.0	Policy Review	12

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 Tornillo ISD full- and part-time employees, contractors, paid or unpaid interns, and other users of government networks. All Tornillo ISD 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.

Tornillo ISD 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.

Tornillo ISD 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 Governmental Entity-implemented security measures.**

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 **Tornillo ISD** will remove and prohibit the covered application.

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

2.4 BRING YOUR OWN DEVICE POLICY

If **Tornillo ISD** has a "Bring Your Own Device" (BYOD) program, then the

Tornillo ISD may consider prohibiting the installation or operation of covered applications on employee-owned devices that are used to conduct government business.

2.5 COVERED APPLICATION EXCEPTIONS

Tornillo ISD 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 **Tornillo 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 **Tornillo ISD** authorizes an exception allowing for the installation and use of a covered application, **Tornillo ISD** must use measures to mitigate the risks posed to the state during the application's use **including**:

- **Measures that the Tornillo ISD deems appropriate for its own policy.**

Tornillo ISD 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 **Tornillo ISD** employees, including interns and apprentices, contractors, and users of state networks. All **Tornillo ISD** 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 **Tornillo ISD** 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 **Tornillo ISD** 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 **Tornillo ISD**

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 Tornillo ISD BYOD program, which may include proactive enrollment in the program.

Tornillo ISD BYOD program prohibits an employee or contractor from enabling prohibited technologies on personal devices enrolled in the Tornillo ISD program.

3.4 SENSITIVE LOCATIONS

Tornillo ISD 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.

3.5 NETWORK RESTRICTIONS

DIR has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, Tornillo ISD 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 Tornillo ISD 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 Tornillo ISD 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 BRING YOUR OWN DEVICE POLICY FOR A GOVERNMENTAL ENTITY NOT SUBJECT TO THE GOVERNOR’S PROHIBITED TECHNOLOGY DIRECTIVE

If a Tornillo ISD is not subject to the Governor’s prohibited technology directive but is subject to Senate Bill 1893, it may also consider prohibiting the installation or operation of prohibited technologies and covered applications on employee-owned devices that are used to conduct government business.

If **Tornillo ISD** has a “Bring Your Own Device” (BYOD) program, then the **Tornillo ISD** shall institute a “Bring Your Own Device” (BYOD) policy requiring the enrollment of these personal devices in the entity’s program before their continued use in conducting governmental business.

3.8 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.

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

4.0 POLICY COMPLIANCE

All Tornillo ISD 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.

Tornillo ISD 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.

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 **Tornillo ISD**.



RE: Fw: Policy Alert: Policy on Covered Applications on District Devices

From Escarsega, Christopher <EscarsegaC@tisd.us>

Date Thu 11/7/2024 11:40 AM

To Steve Sinor <steve@solidborder.com>; Garcia, Carlos <GarciaC@tisd.us>

Some were already being block I added the others and tested, and they are now being block.

TikTok **Yes**

• Kaspersky **Yes**

• ByteDance Ltd. **Just added now**

• Tencent Holdings Ltd. **Just added now**

• Alipay **Just added now**

• CamScanner **Yes**

• QQ Wallet **Yes**

• SHAREit **Yes**

• VMate **Yes**

• WeChat **Yes**

• WeChat Pay **Yes**

• WPS Office **Yes**

From: Steve Sinor <steve@solidborder.com>

Sent: Thursday, November 7, 2024 9:54 AM

To: Garcia, Carlos <GarciaC@tisd.us>

Cc: Escarsega, Christopher <EscarsegaC@tisd.us>

Subject: Re: Fw: Policy Alert: Policy on Covered Applications on District Devices

CAUTION: This email originated from outside TISD organization. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

The following applications need to be added to your Application Block List to ensure that everything is blocked. I believe there are a few in this list that are new, so you need to check your list:

Alipay

tencent (2 apps)

wechat (several apps)

QQ (multiple apps, but not "wallet", you should probably just block all of QQ to be safe, it is a Chinese chat app so you probably don't need it)

Kaspersky (3 apps, at least one is probably new)

Dahua

Huawei

Hikvision (2 apps)

The rest of the list should already be applied to your firewall (URLs, IPs, etc)