Covered Applications and Prohibited Technology

PURPOSE

Establish procedures and administrative regulations for covered applications and prohibited technologies at Temple College.

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.

In addition to TikTok, Temple College may add other software and hardware products with security concerns to this regulation and will be required to remove prohibited technologies that are on the DIR prohibited technology list. Throughout this regulation, "Covered Applications" or "Prohibited Technologies" shall refer to TikTok and any additional hardware or software products added to this regulation in the following addendums.

SCOPE

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 regulation applies to all Temple College full and part-time faculty, staff, and employees, including adjunct faculty, student workers, and any contractor that has access to Temple College's network or is conducting Temple College business. All Temple College employees are responsible for complying with this policy

PROCESS

College-Owned Devices

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

Temple College must identify, track, and control state-owned devices to prohibit the installation or access to all covered applications. This includes the various prohibited applications for mobile, desktop, or other internet-capable devices.

Temple College must 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 unauthorized software from mobile devices.

d. Deploy secure baseline configurations, for mobile devices, as determined by Temple College.

Personal Devices Used for College Business

Employees and contractors may not install or operate prohibited applications or technologies on any personal device that is used to conduct state business. State business includes accessing 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 Temple College's BYOD program, which may include

proactive enrollment in the program.

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

Identification of Sensitive Locations

Sensitive locations must be identified, cataloged, and labeled by Temple College. 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 or BYOD policy may not bring their personal device into sensitive locations. This includes using their unauthorized personal devices to access any electronic meeting labeled as a sensitive location.

Visitors granted access to secure locations are subject to the same limitations as contractors and employees on unauthorized personal devices when entering secure locations.

Sensitive locations at Temple College are to be labeled with a sign on the door indicating that unauthorized access is prohibited and that no cell phones, cameras, or other personal devices will be allowed in the room. Examples of sensitive locations include file and record storage rooms and technology data centers. Devices that adhere to the BYOD policy will be permitted in these spaces.

Network Restrictions

Texas Department of Information Resources (DIR) has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, Temple College will also implement additional network-based restrictions including:

a. Configure firewalls to block access to statewide prohibited services on all technology infrastructures, including local networks, WAN, and VPN connections.

b. Prohibit personal devices with prohibited technologies installed from connecting to agency or state technology infrastructure or state data.

c. Provide a separate network for access to prohibited technologies with the approval of the Chief Information Officer. This network will be labeled as a guest network and will only have access to the public internet connection and will not have access to any internal network resources including other devices on the same network.

Ongoing and Emerging Technology Threats

To provide protection against ongoing and emerging technological threats to the state's sensitive information and critical infrastructure, the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (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.

Temple College will implement the removal and prohibition of any listed technology. Temple College may prohibit technology threats in addition to those identified by DIR and DPS and will add them to Addendum B.

Regulation Compliance

All Temple College employees shall sign a document annually confirming their understanding of the agency's covered applications and prohibited technology policies. This document will be presented along with the mandatory cybersecurity training.

Compliance with this regulation will be verified through various methods, including but not limited to, IT/security system reports and feedback to Temple College leadership.

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

Exceptions

Temple College 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 Temple College 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 Temple College authorizes an exception allowing for the installation and use of a covered application, Temple College must use measures to mitigate the risks posed to the state during the applications use. Temple College must document whichever measures it took to mitigate the risks posed to the state during the use of the covered application.

Exceptions to the ban on prohibited technologies may only be approved by the Chief Information Officer of Temple College. This authority may not be delegated. All approved exceptions to the TikTok prohibition or other statewide prohibited technology must be reported to DIR.

Exceptions to the regulation will only be considered when prohibited technologies are required for a specific business need, such as enabling criminal or civil investigations or sharing information with the public during an emergency. For personal devices used for state business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period of time. To the extent practicable, exception-based use should only be performed on devices that are not used for other state business and on non-state networks. Cameras and microphones should be disabled on devices for exception-based use. Exceptions are found in Addendum C.

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 Temple College.

Addendum A – State-prohibited technologies

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 policy adoption

Prohibited Software/Applications/Developers

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

Prohibited Hardware/Equipment/Manufacturers

- 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.

Covered Applications

- Lemon8
- RedNote

- TikTok or any successor application or service developed or provided by ByteDance Ltd. or an entity owned by ByteDance Ltd.

Addendum B – Local Prohibited Technologies

Technologies added to this list will be prohibited from all Temple College-owned devices and networks.

There are no Local Prohibited Technologies at this time.

Addendum C – Local Exceptions

Exceptions added to this list will be exempt from this policy.

- Student-owned devices will be exempt from this policy while on the TC.Guest and TC.BYOD networks. Access to prohibited services has been blocked on these networks, but student-owned devices with prohibited applications installed will be allowed to use Temple College wireless networks.