# McLennan Community College

## POLICIES AND PROCEDURES

| | | | | |
|---|---|---|---|---|
| Reference: | E-XIV | | Effective Date | 02/05/2025 |
| Subject: | Prohibited Technologies Security Control | | | |
| Source: | President | | | |
| Approval Authority: | President | | Approval Date | 02/05/2025 |
| Approved by Leadership Team: | JEM: | MH: | CE: | LW: |
| History: | Replaced previous policy dated 11/20/2024 | | | |
| Remarks: | | | | |

### Prohibited Technologies Security Control

All state agencies are required 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 policy establishes McLennan Community College's compliance as an entity subject to the directive and/or bill to prohibit the installation or use of covered applications or prohibited technologies on applicable devices.

In addition to TikTok, McLennan Community College may add other software and hardware products with security concerns to this policy and will be required to remove prohibited technologies which are on the DIR prohibited technology list. Throughout this Policy, "Prohibited Technologies" shall refer to TikTok and any additional hardware or software products added to this Policy.

This policy applies to all McLennan Community College employees, contractors, paid or unpaid interns, and users of state networks. All employees are responsible for complying with its terms and conditions.

**College-Owned Devices**

Except where approved exceptions apply, the use or download of prohibited applications or

websites is prohibited on all McLennan Community College owned devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

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

McLennan Community College manages all McLennan Community College owned devices using the security controls listed below:

a. Employees who receive McLennan Community College issued devices are instructed not to install prohibited applications.
b. McLennan Community College issued devices are periodically reviewed to ensure prohibited applications are not installed.
c. Employees who install prohibited applications on McLennan Community College issued devices are subject to disciplinary action.

**Personal Devices Used for McLennan Community College Business**

Employees and contractors are discouraged from installing or operating prohibited applications on any personal devices that is used to conduct McLennan Community College business. McLennan Community College business includes accessing any McLennan Community College owned data, applications, email accounts, non-public facing communications, McLennan Community College email, VoIP, SMS, video conferencing, CAPPS, Texas.gov, and any other McLennan Community College databases or applications.

Access to McLennan Community College owned data and applications shall use secure data encryption and required virtual private network connections.

**Identification of Sensitive Locations**

McLennan Community College presently has no sensitive locations. Sensitive locations are any physical or logical locations containing confidential information to such an extent as to create exceptionally grave damage to the college or an individual.

**Network Restrictions**

McLennan Community College has blocked access to prohibited technologies on the McLennan Community College network. To ensure multiple layers of protection, McLennan Community College will configure agency firewalls to block access to McLennan Community Collegewide prohibited services on all McLennan Community College technology infrastructures, including local networks, WAN, and VPN connections.

# POLICIES AND PROCEDURES

## Ongoing and Emerging Technology Threats

To provide protection against ongoing and emerging technological threats to the McLennan Community College's (as well as other governmental entities') sensitive information and critical infrastructure, DPS and DIR will regularly monitor and evaluate additional technologies posing concerns for inclusion in this policy.

DIR will host a site that lists all prohibited technologies including apps, software, hardware, or technology providers. The prohibited technologies list can be found at Addendum A. New technologies will be added to the list after consultation between DIR and DPS.

McLennan Community College will implement the removal and prohibition of any listed technology. McLennan Community College may prohibit technology threats in addition to those identified by DIR and DPS.

## Policy Compliance

All employees shall sign a document annually confirming their understanding of this policy.

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

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

## Exceptions

Exceptions to the ban on prohibited technologies may only be approved by the President of McLennan Community 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 policy will 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 McLennan Community College 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 McLennan Community College business and on non-McLennan Community College networks. Cameras and microphones should be disabled on devices for exception-based use.

## 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 February 5, 2025.

### Prohibited Software/Applications/Developers

Last updated January 31, 2025

- 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 an entity listed above.

### Prohibited Hardware/Equipment/Manufacturers

Last Updated January 31, 2025

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

# POLICIES AND PROCEDURES

## Covered Applications

Last Updated January 31, 2025

- Lemon8
- RedNote
- TikTok or any successor application or service developed or provided by ByteDance Ltd. Or an entity owned by ByteDance Ltd.