BLINN COLLEGE DISTRICT ADMINISTRATIVE REGULATIONS MANUAL

SUBJECT: *Prohibited Technologies and Covered Applications*
EFFECTIVE DATE: November 7, 2024
BOARD POLICY REFERENCE: CS

PURPOSE

Develop policies and procedures for blocking prohibited technologies and covered applications per Texas Government Code §620 and proclamation of the governor.

SCOPE

This policy applies to all Blinn College District full and part-time employees including contractors, paid and unpaid volunteers, and users of state networks. All College District employees are responsible for complying with the terms and conditions of this policy.

Prohibited Technologies Policy

College District-Owned Devices

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

The College District must identify, track and control College District-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.

The College District must manage all 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 College District.

A covered application is:

A. The social media service TikTok or any successor application or service developed or provided by ByteDance Limited, or an entity owned by ByteDance Limited.
B. A social media application or service specified by proclamation of the governor under Government Code Section 620.005.

Covered Applications Exceptions

The College District 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 College District 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 College District authorizes an exception allowing for the installation and use of a covered application, the College District must use measures to mitigate the risks posed to the state during the application's use

- Restricting what other College District data and/or applications reside with the covered application
- Restricting where the covered application can operate on College District property and networks
- Other measures that the College District deems appropriate

The College District must document whichever measures it took to mitigate the risks posed to the state during the use of the covered application.

Ongoing and Emerging Technology Threats

To provide protection against ongoing and emerging technological threats to the government'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 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 College District will remove and prohibit the covered application.

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

Compliance

The College District will verify compliance with this administrative regulation through various methods, including but not limited to, IT/security system reports and feedback to leadership.

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