Office of the Chancellor

THE TEXAS A&M UNIVERSITY SYSTEM

July 12, 2023

MEMORANDUM

TO: All Chief Information Officers

SUBJECT: The Texas A&M University System's Prohibited Technologies Plan

On December 7, 2022, Governor Greg Abbott required all state agencies to ban the video-sharing application TikTok from all state-owned 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.

The guidance issued by DPS and DIR requires The Texas A&M University System ("system") to remove prohibited technologies which are on the DIR prohibited technology list ("Prohibited Technology") from state-owned devices and block access to prohibited technologies from state-owned networks.

This plan is adopted under the authority of System Policy 29.01, *Information Resources*, and applies to all system employees, contractors and users of system member networks. All system employees, contractors and users are responsible for complying with this plan. In this plan, "prohibit" is to not allow by policy and "prevent" is to have a technical control in place unless an exception exists.

All exceptions to this plan are treated as high residual risk decisions as defined in 1 TAC § 202.75(4)(B) and must be approved by the institution of higher education head and reported to DIR. This authority may not be delegated. Exceptions are limited to the following categories:

- Law enforcement and public safety investigations
- Other investigations and adjudications required by law, regulation or policy
- Enforcement of system-owned intellectual property rights
- Research in which a Prohibited Technology is critical to the project and an approved technology control plan is in place to protect campus research security, data and networks

Members are directed to implement any necessary administrative, operational or technical security controls to accomplish the following:

1. MANAGING MEMBER-OWNED DEVICES AND NETWORKS

1.1. Except where approved exceptions apply, members must prohibit the use or download of prohibited technologies on all member-owned devices, including mobile phones, tablets, desktop and laptop computers, and other internet capable devices.

1.2. Members must identify, track, and control member-owned devices to prevent the installation of or access to all prohibited applications.

1.3. Members must manage all member-issued mobile devices by implementing the following security controls:

1.3.1. Restricting access to prevent the installation of prohibited applications;

1.3.2. Maintaining the ability to remotely wipe non-compliant or compromised mobile devices;

1.3.3. Maintaining the ability to remotely uninstall prohibited applications from mobile devices, and

1.3.4. Deploying security baseline configurations for mobile devices as determined by the member.

1.4. Members must configure security protection technologies (such as firewalls, endpoint protection, and email security gateways) to prevent communication with prohibited applications on all member technology infrastructure.

1.5. Members must prohibit personal devices with prohibited hardware from connecting to member technology infrastructure, specifically local networks and VPN connections. Connections to public-facing member technology through the Internet (such as the member's public website or publicly available applications) are excluded from this prohibition.

1.6. Members must implement the removal and prohibition of any prohibited technology listed on the DIR website at https://dir.texas.gov/information-security/prohibited-technologies, including any future additions or removals to the list.

1.7. Members may provide a separate logical or physical network for access to prohibited technologies with the approval of the member chief executive officer.

2. MANAGING PERSONAL DEVICES

2.1. Member employees and contractors are prohibited from installing or operating prohibited technologies on any personal devices that are used to conduct state business.

2.2. Members must include the employee/contractor/user provisions of this plan in their rules of behavior and require all employees, contractors and users of member-owned networks to acknowledge the rules of behavior as part of their annual security awareness training.

3. IDENTIFICATION OF SENSITIVE LOCATIONS

3.1. Members must identify, catalog, and label locations designated as “sensitive locations”. Sensitive locations are defined as any location, physical or logical, that are used to discuss Confidential or Internal Use information of a sensitive nature that must be protected from unauthorized disclosure or public release.

3.2. Information owners will identify the information under their control that requires protection from unauthorized disclosure which will be only discussed within sensitive locations.

3.3. Members must prohibit devices with prohibited technology from entering sensitive locations, including any electronic meeting labeled as a sensitive location, when discussions involving sensitive information take place.

3.4. Visitors granted access to sensitive locations are subject to the same limitations as employees and contractors on prohibited technology-enabled devices when entering sensitive locations.

Mark A. Stone, Ph.D.
System Chief Information Officer

cc: Chief Executive Officers
Chief Financial Officers