Procedure III.3010.A.d, Prohibited Technologies

Associated Policy
Policy III.3010.A, Information Resources

1. Purpose

On December 7, 2022, the Governor of Texas 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 (Texas DPS) and the Texas Department of Information Resources (Texas DIR) to develop a plan providing state agencies guidance on managing Personal Devices used to conduct state business.

This Procedure refers to the College's "Security Plan for Prohibited Technologies" and "Prohibited Technologies Security Policy" as required by Texas State Law. In addition to TikTok, the College may add other software and hardware products with security concerns to this Procedure and will be required to remove Prohibited Technologies which are on the Texas DIR Prohibited Technology list. Throughout this Procedure, "Prohibited Technologies" shall refer to TikTok and any additional hardware or software products added to this Procedure.

2. Applicability

This Procedure applies to all College Information Resources and the Users of such Information Resources, in any form, and is intended to be broad enough to include all Users.

3. Laws, Regulations, and Standards

The College is required to comply with Texas State Laws and Regulations. Specifically, Chapter 620 of Texas Government Code Title 6 Subtitle A provides specific guidance for the use of certain social medial applications and services. Sec.620.001(1)(A) specifies the social media service TikTok or any successor application or service developed or provided by ByteDance Limited, or an entity owned by ByteDance Limited.

4. List of Prohibited Technologies

Texas DIR will host a site located at located at https://dir.texas.gov/information-security/prohibited-technologies that lists all Prohibited Technologies including apps, software, hardware, or technology providers. The College will implement the removal and prohibition of any listed technology. The College may prohibit technology threats in addition to those identified by Texas DPS and Texas DIR.

5. Associated Program Controls

The following Program Controls associated with this Procedure are:

RA Risk Assessment Control Family

- RA-3 Risk Assessment
- RA-3(1) Risk Assessment | Supply Chain Risk Assessment
- RA-5 Vulnerability Monitoring and Scanning
- RA-5(2) Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be
- Scanned
- RA-7 Risk Response

6. Roles and Responsibilities

The roles and responsibilities as defined by the Information Security Program are described in Procedure III.3010.A.a, Information Security Program. Described below are additional roles and responsibilities that pertain to this Procedure.

a. **The Office of Cybersecurity (OCS)** performs the following duties**:**

- Schedules and prioritizes Cybersecurity Risk Assessments.
- Requests information from College Users related to their collection and use of Protected Data.
- Conducts Cybersecurity Risk Assessments.
- Processes and follows up on requested exceptions to the College's Policies and Procedures.
- Participates in the Cybersecurity Risk Management program, including identification of assets and services, allocation of resources, risk prioritization, risk acceptance, and implementation of risk treatment plan.

b. **College User(s)** is an individual, automated application, or process that is authorized by the College to access an Information Resource. Includes, but is not limited to, all College students, faculty, staff, contractors, guests, departments, and any individual, application, or process that accesses and or uses the College's Information Resources.

7. College Devices used to conduct College Business

The use or download of Prohibited Technologies is prohibited on all College-owned devices, except where approved exceptions apply. Please refer to Section 9 of this Procedure on Exceptions.

8. Personal Devices used to conduct College Business

Personal Devices may be used by all College Users to conduct College Business, and the College will include security considerations to protect the College's network and data from traffic related to Prohibited Technologies. However, the following limitations apply to this granted use:

a. Access to Information Resources when using a Personal Device is limited to Information Resources protected by Multi-factor Authentication (MFA) and defense in depth.

b. Students are restricted to only use a Personal Device that is privately owned or leased by the Student or a member of the Student's immediate family or the Student's ISD or Academy.

c. Users who are employed or contracted by the College must not install or operate Prohibited Technologies on any Personal Device that is used to conduct College Business.

9. Exceptions

Exceptions to this Procedure will only be considered when the use of Prohibited Technologies is required for a specific need to conduct College Business, such as enabling criminal or civil investigations or for sharing of information to the public during an emergency.

Requests for exceptions must be submitted as a support ticket to the ITS Help Desk to the attention of the Chief Information Security Officer (CISO). Once reviewed, the request and the CISO's recommendation will be submitted to the CTIO and Strategic Leadership Team (SLT) for review. Exceptions to the ban on Prohibited Technologies may only be approved by the Chancellor. This authority may not be delegated.

All approved exceptions to the TikTok prohibition or other statewide Prohibited Technologies must be reported to Texas DIR by the CISO.

10. Implementation of the Security Plan

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

Objective 1: Prohibit the download or use of Prohibited Technologies on any College-issued device.

The College is required to identify, track, and control 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. Specifically, the College must manage all College-issued mobile devices by implementing the following security controls:

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 the College.

Objective 2: Prohibit employees and contractors from conducting College Business on Prohibited Technology enabled Personal Devices.

The College may establish a Bring Your Own Device (BYOD) program if there is a justifiable need for the use of Personal Devices to conduct College Business. Such program must consider the following:

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 College-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.

Sensitive locations must be identified, cataloged, and labeled by the College as soon as reasonably practicable. 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 and State Laws. Data rooms, data closets, emergency operations center and any other location are also regarded as sensitive locations. Exterior signage will be used to identify or label sensitive locations.

Unauthorized devices such as personal cell phones, tablets, or laptops may not enter sensitive locations, which includes any electronic meeting labeled as a sensitive location. Visitors, to include students, granted access to sensitive locations are subject to the same limitations as College Users on unauthorized personal devices when entering sensitive locations.

Objective 4: Implement network-based restrictions to prevent the use of Prohibited Technologies on the College networks by and Prohibited Technology-enabled personal device.

To ensure multiple layers of protection, the College will implement additional network-based restrictions to include:

- Configure College firewalls to block access to statewide prohibited services on all College technology infrastructures, including local networks, WAN, and VPN connections. Ensure periodic evaluation of rules as URLs, domains, and IP addresses may change frequently.
- Prohibit Personal Devices with Prohibited Technologies installed from connecting to College technology infrastructure or data.
- Provide a separate network for access to Prohibited Technologies with the approval of the Chancellor.

11. Ongoing and Emerging Technology Threats

To provide protection against ongoing and emerging technological threats to Texas State's sensitive information and critical infrastructure, Texas DPS and Texas DIR will regularly monitor and evaluate additional technologies posing concerns for inclusion in this Procedure.

12. Compliance

All College Users shall annually confirm their understanding of this Procedure. Confirmation will be included in the College's Annual Cybersecurity Awareness training and added to the Acceptable Use of Information Resources Procedure.

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

College Users found to have violated this Procedure may be subject to disciplinary action, including termination of employment.

13. Definitions

The terms referenced in this Procedure are outlined in **Procedure III.3010.A.a, Information Security Program**, Section 14. Definitions.

Date of SLT Approval	February 15, 2024
Effective Date	February 15, 2024
Associated Policy	Policy III.3010.A, Information Resources
Primary Owner of Policy Associated with the Procedure	Chief Technology Innovations Officer
Secondary Owner of Policy Associated with the Procedure	Chief Information Security Officer