SECTION: Information Technology **NUMBER: 07.A.12**

AREA: Computing Services

SUBJECT: Prohibited Technologies and Covered Applications (Interim)

---

1. PURPOSE

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. Effective June 14, 2023, Texas Government Code, Chapter 620 requires all state agencies to prohibit the use or installation of covered applications on governmental entity devices, which include devices owned or leased by an institution of higher education.

2. SCOPE

This policy applies to all University of Houston System (UHS) full and part-time employees, students, contractors, paid or unpaid interns, volunteers, guests, visitors, and users of UHS networks. For purposes of this policy, the term "UHS" encompasses the University of Houston System and its universities.

3. DEFINITIONS

3.1. Covered Application – As defined in Texas Government Code, Section 620.001(1), the social media service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited, or a social media application or service specified by proclamation of the governor under section Texas Government Code, Section 620.005.

3.2. Prohibited Technologies – Any technologies listed on the DIR Prohibited Technologies List, including, but not limited to, certain software, hardware, companies, telecommunications devices, and equipment.

3.3. Sensitive Location – Any area with specific compliance requirements mandating limited access, such as a SCIF (sensitive compartmentalized information facility).

4. POLICY

4.1. UHS-Owned Devices

Except where approved exceptions apply, the use or installation of Covered Applications or Prohibited Technologies is prohibited on all UHS-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

UHS will identify, track, and control UHS-owned devices to prevent the installation of or access to Covered Applications and Prohibited Technologies or remove Covered Applications and Prohibited Technologies on UHS-owned devices. This includes the various Covered Applications and Prohibited Technologies for mobile, desktop, or other internet capable devices.

All UHS-issued devices will be managed using a solution approved by UHS Information Security.

Each UHS university information technology department will manage all university-issued devices by implementing the security controls listed below:

a. Restrict access to app stores or non-authorized software repositories to prevent the installation of Covered Applications and Prohibited Technologies.
b. Maintain the ability to remotely wipe non-compliant or compromised devices.
c. Maintain the ability to remotely uninstall unauthorized software from devices.
d. Deploy secure baseline configurations as determined by UHS Information Security.

4.2. Personally Owned Devices Used For UHS Business

Employees and contractors must not install or operate Covered Applications or Prohibited Technologies on any personally owned device that is used to conduct university business.

4.3. Identification of Sensitive Locations

Sensitive Locations will be identified, cataloged, and labeled by UHS. Devices such as personal cell phones, tablets, or laptops not compliant with this policy regarding Covered Applications and Prohibited Technologies may not enter identified Sensitive Locations.

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

4.4. Network Restrictions

4.4.1 UHS will implement network-based restrictions by:

a. Configuring UHS firewalls to block access to Covered Applications and Prohibited Technologies on all UHS technology infrastructures, including local networks, WAN, and VPN connections; and
b. Providing a separate network for access to Covered Applications and Prohibited Technologies when approved by either the UHS Chancellor or applicable university president.

4.4.2 Personally owned devices with Covered Applications and Prohibited Technologies are prohibited from connecting to UHS technology infrastructures.

4.5. Purchasing Restrictions

UHS universities will not purchase or reimburse the purchase of any Covered Applications or Prohibited Technologies.

4.6. Ongoing and Emerging Technology Threats

UHS may add other software and hardware products with security concerns to this policy. UHS will remove and prevent installation and use of Prohibited Technologies and Covered Applications on UHS-owned devices as they are added on the DIR Prohibited Technologies list (https://dir.texas.gov/information-security/prohibited-technologies or specified by proclamation of the governor.

5. EXCEPTIONS

5.1. Covered Application Exceptions

UHS may permit exceptions authorizing the installation and use of a Covered Application on a UHS-owned device for the purposes of:

a. Providing law enforcement; or
b. Developing or implementing information security measures.

Exceptions must be approved by either the UHS Chancellor or applicable university president under the procedures described in Section 5.3 below, and exception requests must have documentation describing measures that will be used to mitigate the risks posed during the use of the Covered Application.

5.2. Prohibited Technologies Exceptions

UHS may permit exceptions authorizing the installation and use of Prohibited Technologies on UHS-owned devices for the purposes of:

a. Law enforcement and public safety;
b. Investigations and adjudications required by law, regulation, or policy;
c. Enforcement of university-owned intellectual property rights;
d. Research when the researcher uses Prohibited Technologies as part of their field of study, but only if such use would be conducted from university-issued devices used solely for Prohibited Technologies and would not be used for any other university purpose or to access any other university service;
e. Teaching when faculty use Prohibited Technologies as part of their curriculum, but only if such use would be conducted from university-issued devices used solely for Prohibited Technologies and would not be used for any other university purpose or to access any other university service; or
f. Other specific business needs as approved.

Exceptions must be approved by either the UHS Chancellor or applicable university president under the procedures described in Section 5.3 below. This authority may not be delegated. All approved Prohibited Technologies exceptions must be reported to DIR.

5.3. All exception requests must be submitted to UHS Information Security for review. UHS Information Security will submit the exception request to the UHS Chancellor or applicable university president for approval and report the exception to DIR as required.

6. POLICY COMPLIANCE

All employees will annually confirm their understanding of this policy.

7. REVIEW AND RESPONSIBILITY

Responsible Party: Senior Associate Vice Chancellor for Information Technology

Review: Every five years

8. APPROVAL

Approved: /*Raymond Bartlett*/
Senior Vice Chancellor for Administration and Finance

/*Renu Khator*/
Chancellor

Date: November 13, 2024