TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

Operating Policy and Procedure

HSC OP: 56.06, **Prohibited Technologies**

PURPOSE: To address the requirements set forth by the Governor of Texas, (12/7/2022)[1] to protect critical state infrastructure and to comply with the Lone Star Infrastructure Protection Act[2], TTUHSC is adopting this Prohibited Technologies Policy.

All state agencies are prohibited from using of the video-sharing application TikTok on state-owned and state-issued devices or on networks managed by TTUHSC. TTUHSC reserves the right to add software and hardware considered to pose security risks to a list of prohibited technologies in accordance with the state of Texas's continually updated list of identified technologies.

DEFINITION As outlined in the TTUHSC IT Authorized and Unauthorized Hardware/Software Standard, Prohibited Technologies include, but are not limited to:

i. Any technologies that are not properly licensed;
ii. Any technologies that violate federal, state, or local laws or TTUHSC policies;
iii. Any technologies that are considered by the state government of Texas to be a threat to local, state, or national security; or
iv. Any technologies identified on the Department of Information Resources (DIR)'s Prohibited Technologies page.

SCOPE This policy applies to all TTUHSC full and part-time employees including contractors, paid or unpaid interns, and users of state networks. All TTUHSC employees are responsible for complying with the terms and conditions of this policy.

REVIEW: This OP will be reviewed annually by the TTUHSC President.

TABLE OF CONTENTS

POLICY

[1] https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_1.pdf
[2] Texas Legislature Online SB 2116 summary

POLICY:

1. TTUHSC-Managed Devices

The use or download of Prohibited Technologies is not permitted on TTUHSC-managed devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

TTUHSC must identify, track, and securely manage state-owned devices to prohibit the installation of or access to Prohibited Technologies. This monitoring includes prohibited applications for mobile, desktop, or other internet-capable devices.

TTUHSC must manage all state-issued mobile devices by implementing the security controls listed below:

a. Restricting access to Prohibited Technologies.

b. Maintaining the ability to remotely wipe non-compliant or compromised TTUHSC-managed mobile devices.

c. Maintaining the ability to remotely uninstall un-authorized software from TTUHSC-managed mobile devices.

d. Deploying secure baseline configurations, for TTUHSC-managed mobile devices, as determined by TTUHSC.

2. Personal Devices Used for TTUHSC Business

TTUHSC business includes any interaction that requires access to or use of TTUHSC-owned or managed networks, data, applications, email accounts, non-public facing communications, email, VoIP, SMS, or video conferencing.

Employees and contractors may request that their device be enrolled in the TTUHSC's Bring Your Own Device (BYOD) program which ensures endpoint management on all devices used for TTUHSC business. Employees and contractors are required to remove all Prohibited Technologies from any personal device that has been approved for TTUHSC business.

3. Identification of Sensitive Locations

A sensitive location is any area, 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 or state law.

a. Non-TTUHSC-managed devices such as personal cell phones, tablets, or laptops that have Prohibited Technologies may not enter locations labeled as sensitive including any electronic meeting labeled as a sensitive location.

b. Visitors granted access to secure locations are subject to the same limitations as contractors and employees and may not bring unauthorized personal devices that have Prohibited Technologies into secure locations.

4. Network Restrictions

TTUHSC will implement additional network-based restrictions to include:

a. Firewalls configured to block access to Prohibited Technologies on all institutional technology infrastructures, including local networks, WAN, and VPN connections.

b. Not allowing devices with Prohibited Technologies to connect to TTUHSC networks.

5. Ongoing and Emerging Technology Threats

a. TTUHSC will regularly monitor and evaluate additional technologies posing concerns following recommendations from DIR, DPS, FDA, and CISA.

b. All TTUHSC Prohibited Technologies inclusive of state-mandated Prohibited Technologies, can be found in the TTUHSC IT Authorized and Unauthorized Hardware and Software Standard.

c. TTUHSC IT is responsible for blocking or removing any Prohibited Technologies.

6. Purchasing Restriction

TTUHSC will not purchase or reimburse the purchase of any Prohibited Technologies, unless an exception has been approved.

7. Policy Compliance

a. All employees must annually acknowledge and confirm their understanding of this policy.

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

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

8. Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. TTUHSC reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

9. Exceptions

Appeals to the policy will only be considered when the use of Prohibited Technologies is required for a specific business need and will be evaluated on a case-by-case basis.

a. To the extent practicable, exception-based use should only be performed on devices that are not used for other TTUHSC business and on non-TTUHSC networks.

b. Exceptions to the ban on Prohibited Technologies may be approved by the President of TTUHSC. This authority may not be delegated.

c. All approved appeals to this policy will be reported to DIR.

10. Relevant Policies

The following TTUHSC policies support the requirements of this HSC OP by implementing controls that ensure state-recognized security baselines for information and information resource management as it applies to the above-mentioned Prohibited Technologies:

- HSC OP 56.01 Acceptable Use
- TTUHSC IT Policy 56.07 Insider Threat Program
- TTUHSC IT Policy 56.12 Configuration Management
- TTUHSC IT Policy 56.24 Management of Information Resource Assets
- TTUHSC IT Policy 56.29 Third-Party Risk Management
- TTUHSC IT Policy 56.35 Media Protection
- TTUHSC IT Threat Awareness Program (available by request)
- STANDARD: Authorized and Unauthorized Hardware and Software

- STANDARD: Vulnerability Management

11. Document Details

Approval and Ownership

Approved By	Lori Rice-Spearman, Ph.D.
Title	President Texas Tech University Health Sciences Center
Approval Date	07/12/2023
Owner(s)	TTUHSC Office of Information Technology

Revision History

Version	Description	Date Reviewed	Date Submitted for Publishing	Reviewer(s)
1.0	Initial version.	02/14/2023	07/12/2023	TTUHSC IT ISO
1.5	Revision	01/16/2026	01/16/2026	CIO, ISO
1.5.1	Supplementary information added	04/16/2026	04/17/2026	CIO, ISO