The University of Texas Rio Grande Valley
Information Security Office

Prohibited Technology and Covered Applications

Section 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. On February 14, 2023, The University of Texas Office of General Counsel issued The University of Texas System's Prohibited Technologies Security Policy ("Prohibited Technology Policy"). Following the issuance of the Governor's directive and the Prohibited Technology Policy, the 88th Texas Legislature passed Senate Bill 1893, which prohibits the use of covered applications on governmental entity devices.

Section 2. Scope and Application

2.1 This policy follows the requirements of The University of Texas System and applies to (1) The University of Texas Rio Grande Valley (2) Prohibited Technologies, defined as all technologies identified in or as a result of (a) the Governor's December 7, 2022 directive or any subsequent directive of the Governor, or (b) Chapter 620 of the Texas Government Code (including covered applications as defined therein) or any subsequent Texas law or regulation. This policy replaces all previous prohibited technology policies enacted pursuant to the Governor's December 7, 2022 directive.

2.2 This policy must be complied with by all System full- and part-time employees, contractors, paid or unpaid interns, apprentices, and other users of government-owned or leased devices or government networks (collectively, "UTRGV Personnel").

2.3 The Prohibited Technologies include, but are not limited to, the following:

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 (1) proclamation of the Governor under Government Code Section 620.005 or (2) the Department of Information Resources and the Department of Public Safety under Government Code Section 620.006.

c) Any Prohibited Technologies made available through application stores for mobile, desktop, or other internet capable devices.

Section 3. Prohibited Technologies on Government-Owned or Leased Devices

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

3.2 UTRGV will manage its operations and identify, track, and manage all government-owned or -leased devices including mobile phones, tablets, laptops, desktop computers, or any other internet-capable devices to:

a) Prohibit the installation of Prohibited Technologies.

b) Prohibit the use of Prohibited Technologies.

c) Halt the use of Prohibited Technologies that were obtained or used by UTRGV prior to the effective date of the Governor's December 7, 2022 directive or of Chapter 620 of the Texas Government Code.

d) Remove Prohibited Technologies that were installed or used on governmentowned or -leased devices, networks, and computer systems prior to the effective date of the Governor's December 7, 2022 directive or of Chapter 620 of the Texas Government Code.

e) Halt the use of and remove a technology from government-owned or -leased devices, networks, and computer systems once it is identified as a Prohibited Technology.

3.3 UTRGV information technology and information security offices will manage all government-owned or leased devices by implementing the security measures listed below:

a) Document, maintain, and implement procedures to restrict access to "app stores", websites, or other unauthorized software repositories to prevent the installation or use of Prohibited Technologies. Such procedures will be both procedural (for example, inclusion and enforcement of appropriate written terms in the UTRGV acceptable use policies) and technological (for example, establishing technical safeguards to prevent government-owned or leased devices from accessing, downloading, installing, or operating Prohibited Technologies.)

b) Establish, implement, and maintain the ability to remotely wipe Prohibited Technologies from non-compliant or compromised devices, networks, and computer systems.

c) Establish, implement, and maintain the ability to remotely uninstall and disable Prohibited Technologies from devices, networks, and computer systems.

d) Deploy secure baseline configurations for mobile devices as determined by UTRGV.

e) Develop, maintain, and implement audits of government-owned or leased devices, networks, and computer systems to ensure compliance with this policy.

3.4 UTRGV information technology and information security offices will implement the above security measures to the extent possible and practical through the use of technologies that currently exist, or which become available in the future.

Section 4. Personal Devices Used For State Agency Business

4.1 UTRGV Personnel may not install or operate prohibited applications or technologies on any personal device that is used to conduct state business, which includes using the device to access any state-owned data, applications, email accounts, non-public facing communications, state email, VoIP, SMS, video conferencing, CAPPS, Texas.gov, and any other state databases or applications.

4.2 According the UTS 200, to the extent UTRGV has a "Bring Your Own Device" (BYOD) program, then there must be a "Bring Your Own Device" (BYOD) policy governing that program that (1) requires the enrollment of all personal devices in the program before the continued use of those personal devices in conducting governmental business and (2) prohibits the installation or operation of Prohibited Technologies on any personal devices that are used to conduct government business. UTRGV is instituting a BYOD and Mobile Device Management Program that will comply with this policy, UTS-165, UTS 200, and aligns with the intent of the GLBA and HIPAA Safeguard Rules. Effective the Summer of 2026 UTRGV will institute a new and improved BYOD policy for the institution.

Section 5. Sensitive Locations

5.1 UTRGV information security offices and police departments will identify, catalogue, label, and develop procedures for use of all sensitive locations at UTRGV campuses and buildings. A sensitive location is any location, physical or logical (such as video conferencing, or electronic meeting rooms), during the period that location is used to display or 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, such as a SCIF (sensitive compartmentalized information facility).

5.2 UTRGV Personnel whose personal device, including their personal cell phone, tablet, or laptop, is not compliant with this Prohibited Technology policy may not bring their personal device into a sensitive location or use their personal device to otherwise access a sensitive location. This includes using their unauthorized personal device to access any electronic meeting or discussion taking place in a sensitive location, including via remote access.

5.3 Visitors granted access to sensitive locations are subject to the same obligations and limitations as UTRGV Personnel. If a visitor is granted access to a sensitive location and their personal device has Prohibited Technology installed on it, then the visitor must leave their unauthorized personal device at an appropriate location that is not identified as sensitive as determined by the UTRGV information security office or police department governing that secured location.

Section 6. Network Restrictions

DIR has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, UTRGV must also implement additional network-based restrictions, which include:

a) Configuring System firewalls to block access to Prohibited Technologies on all UTRGV technology infrastructures, including local networks, WAN, and VPN connections.

b) Prohibiting personal devices with Prohibited Technologies installed from connecting to UTRGV, UT System or state technology infrastructure or state data.

c) With the approval of the President, provide a separate network that allows access to Prohibited Technologies to the extent necessary for an Prohibited Technology exception under Section 8 of this policy.

Section 7. Ongoing and Emerging Technology Threats

7.1 To provide protection against ongoing and emerging technological threats to the government's sensitive information and critical infrastructure, DPS and DIR will regularly monitor and evaluate additional social media applications or services that pose a risk to this state.

7.2 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 as Prohibited Technologies subject to this policy items that are on this DIR list or items that are otherwise identified by the Governor.

7.3 If the Governor identifies an item as a Prohibited Technologies subject to this policy, then UTRGV will ensure that such an item is addressed in compliance with this policy, including removal and prohibition of that item as required by this policy.

7.4 UTRGV and UT System may also identify social media applications, services, software, hardware, or other technologies as Prohibited Technologies in addition to those specified by proclamation of the Governor or identified by DPS and DIR.

Section 8. Prohibited Technology Exceptions

8.1 UT System and UTRGV have authorized the following exceptions allowing the installation and use of a Prohibited Technology on government-owned or -leased devices or on personal devices subject to a BYOD program consistent with the authority provided by Government Code Chapter 620 to the extent necessary for:

1) Providing law enforcement (including but not limited to land management security and safety);

2) Public safety investigations or other investigations and adjudications required by law, regulation or policy;

3) Developing or implementing information security measures;

4) Enforcement of UTRGV-owned intellectual property rights; or

5) Research (including but not limited to agricultural research) in which a covered technology is critical to the project and an approved technology control plan is in place to protect campus research security, data and networks.

8.2 To the extent UTRGV implements one of these exceptions allowing the installation and use of a Prohibited Technology then the exception must be documented in writing, including the measures to be undertaken to mitigate the risks posed to the state during the Prohibited Technology's use.

Such exception documentation:

a) must include identification of the UTRGV Personnel or Students that are allowed to install and use the Prohibited Technology subject to the exception,

b) must be approved by (i) the applicable UTRGV Office of Department of Police if related to providing law enforcement, (ii) the UTRGV Chief Information Security Officer if related to developing or implementing information security measures, (iii) the UTRGV Chief Research Officer if related to research in which a covered technology is critical to the project, or (iv) the UTRGV Chief Legal Officer if related to (A) enforcement of System-owned intellectual property rights or (B) public safety investigations or other investigations and adjudications required by law, regulation or policy,

c) all exemption requests must also be approved by the Chief Information Security Officer with (b)(ii) requests being countersigned by the Chief Legal Officer,

d) emergency or exigent circumstance investigations or security counter measures can be directly approved by either the CISO or the Chief of Police with follow up review and approval by the appropriate applicable approver,

e) no exception will last for more than one year. Exceptions requiring renewal must be re-evaluated, including control plan updates, and approved per this policy,

f) must be maintained in the information security office and reviewed annually in a report to the UTRGV President, and

g) must be reported to the UTRGV President, DIR, the System Vice Chancellor, and General Counsel once authorized and as required.

Section 9. Policy Compliance

9.1 All UTRGV Personnel shall complete annual information security training confirming their understanding of this UTRGV Prohibited Technology and Covered Applications policy.

9.2 UTRGV's information security office will verify compliance with this policy through various methods, including but not limited to, IT/security system reports and feedback to leadership.

9.3 Any UTRGV Personnel found to have violated this policy may be subject to disciplinary action, including termination of employment.

Section 10. Policy Review

This policy will be reviewed and updated as necessary to reflect changes in state law, additions to Prohibited Technologies identified under Government Code Sections 620.005 or 620.006, updates to the prohibited technology list posted to DIR's website, or to suit the needs of System.

Resources

- UT System Policy (UTS) 165
- UT System Policy (UTS) 200

Applicable Law and Regulation

- Governor's Directive, December 7, 2022
- Texas Government Code, Chapter 620, Use of Certain Social Media Applications and Services on Governmental Entity Devices Prohibited
- Texas Department of Information Resources - Covered Applications and Prohibited Technologies website

Responsible UTRGV Office

Information Security Office

Contact Information

Questions of concerns should be directed to the Information Security Office by emailing is@utrgv.edu or calling 956-665-7823.

Effective Date

February 2026

Revision History

Version	Date	Description	Author
1.0	January 29, 2025	Created document	
2.0	February 2026	Updated document	

Approval History

Version	Date	Title	Name
1.0	January 29, 2025	Chief Information Security Officer	Kevin Crouse
2.0	February 2026	Chief Information Security Officer	Kevin Crouse