Standards for Technologies Prohibited by Regulation

Purpose

This standard establishes (1) a non-exhaustive record of technologies and technology service providers from which the Institute is prohibited from using and/or acquiring and (2) a non-confidential explanation of technical and administrative controls implemented in the furtherance of related compliance goals. Prohibitions highlighted in this standard correspond to state and federal laws, directives, executive orders, and other regulatory requirements applicable to the Institute. The absence of an otherwise prohibited item from this Standard does not imply a means by which the item is authorized.

The contents of this standard are additive overlays that incorporate, detail, and extend requirements set by the Texas State University System (TSUS) Information Technology Policies, institutional policies, other institutional standards, procedures, and guidelines, and additional prohibitions, such as the "Debarred Vendor List" maintained by the Texas Comptroller of Public Accounts.

Pursuant to Sec. 552.139 of Texas Government Code ("Public Information"), some descriptions of technical security controls, procedures, and practices will be abbreviated to avoid disclosure of confidential information pertaining to the security posture of the Institute's information resources.

Scope

This standard generally applies to all Institute-owned information systems, devices, networks, and other information resources that are within the custodianship of the Institute regardless of location. As detailed within, certain sections of this standard may also be applicable to Institute personnel (e.g., Institute officers, employees, contractors), locations (e.g., campuses, properties), and some personally owned devices (e.g., those used to conduct state or Institute Business).

Summary

This section provides an overview of the requirements of this standard. This summary is provided for reference purposes and does not take the place of the full text below.

- Prohibited Technologies and Covered Applications designated by the State of Texas are prohibited on Institute-owned devices.
- Prohibited Technologies and Covered Applications will be blocked on Institute networks.
- The Institute will enhance management capabilities for Institute-owned devices.

- This standard includes procedures for addressing technologies prohibited by regulation in use by the Institute.
- No Exceptions may be authorized for Covered Applications other than those listed in this standard.
- Exceptions to Prohibited Technologies may only be granted by the Institute's president.

Definitions

Terms used in this standard have the meaning ascribed in the Institute's Information Resources Policies unless otherwise clarified in this section.

- **Covered Application**: A social media application or service specified by proclamation of the governor under Section 620.005 including (1) the social media service TikTok or any successor application or service developed or provided by ByteDance Ltd. or an entity owned by ByteDance Ltd., (2) Lemon8, and (3) RedNote.
- **DIR**: Initialism for the Texas Department of Information Resources
- **DPS**: Initialism for the Texas Department of Public Safety
- **Institute Business**: Employees or contractors accessing component-owned information resources including, but not limited to, data, information systems, email accounts, non-public facing communications, telecommunication systems, and video conferencing.
- **Mobile Device Management (MDM)**: The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices.
- **Personnel**: Employees or contractors of the Institute, including faculty, staff, interns, and contractors.
- **Prohibited Technology**: Any technologies listed on the DIR's Prohibited Technologies List, including, but not limited to, certain software, hardware, companies, telecommunications devices, and equipment.
- **Sensitive Location**: Any physical or logical (such as video conferencing or electronic meetings) location designated by the TSUS or a component institution that is routinely used by Personnel to discuss confidential or sensitive information.
- **Unauthorized Devices**: Devices containing prohibited technologies regardless of ownership (e.g., personally owned smart phones with a Prohibited Technology installed).

Technologies Prohibited by The State of Texas

Regulatory Source: Prohibited Technologies

On February 6, 2023, the Governor released a model plan as required by a December 7, 2022, directive banning all state agencies from using TikTok on government-issued devices. This model plan included additional prohibited technologies and detailed objectives intended to protect the state's information resources and infrastructure. The model plan requires each state agency to develop its own policies and procedures to implement the plan and its objectives.

To learn more, refer to the following pages:

- Governor's December 7, 2022, Announcement
- Governor's December 7, 2022, Directive
- Governor's February 6, 2023, Announcement
- DIR's List of Covered Applications and Prohibited Technologies
- Texas State University System's Technologies Prohibited by Regulation Policy

Regulatory Source: Covered Applications

Effective June 14, 2023, Texas Government Code Chapter 620 requires state agencies to prohibit the installation or use of Covered Applications on any device owned or leased by the governmental entity and requiring the removal of covered applications from those devices. Covered Applications are social media applications or services specified by proclamation of the Governor under Sec. 620.005.

To learn more, refer to the following pages:

- Texas Government Code Chapter 620. Use of Certain Social Media Applications and Services on Governmental Entity Device Prohibited
- The TSUS Technologies Prohibited by Regulation Policy
- Governor's January 31, 2025, Proclamation

Prohibition Statements

All Institute Personnel are prohibited from:

- Downloading or using any Prohibited Technologies or Covered Applications on Institute-owned devices;
- Conducting Institute Business on personally owned devices with Prohibited Technologies installed;
- Entering Sensitive Locations with a Prohibited Technology-enabled personal device; and/or
- Acquiring or reimbursing the purchase of Prohibited Technologies.

Exceptions

Exceptions for Covered Applications

Exceptions for Covered Applications may only be approved to enable law enforcement or information security measures. No other exceptions may be authorized for Covered Applications.

Exceptions for Prohibited Technologies

Pursuant to the Governor's directive, exceptions for Prohibited Technologies may be approved only by the Institute's president.

Exceptions for Investigations

The following exceptions are legitimate uses of Prohibited Technologies for the express purpose of performing investigations required by state, federal, or industry regulations:

- Law-enforcement investigations
- Cybersecurity incident investigations
- Student investigations conducted by or authorized by the Dean of Student Services
- Title IX and other discrimination investigations
- Legal Discovery

Exceptions for Severance of Prohibited Technologies

The following exception allows business units, in coordination with the Information Security Officer, to perform data retrieval, account configuration(s), and other activities necessary to reduce the risk of cyber-attacks:

- Temporary maintenance of dormant, high-value data or accounts already in use on a prohibited technology

Exceptions: Residential Internet Services

The following exception is considered a legitimate use of prohibited technologies for the express purpose of providing Internet services to residents' personal devices while they are living in Institute housing:

- Institute residential Internet services transiting through a separate network and used exclusively by residents on personal devices for personal use unrelated to Institute Business.

Enforcement through Security Controls

Technical Controls

A series of technical controls will be used to enforce the prohibition of technologies subject to this standard. Technical controls include, but may not be limited to, the following:

- All Institute-owned devices will be managed to detect and remove Prohibited Technologies and Covered Applications.
- All Institute-owned mobile devices will be enrolled in Mobile Device Management software.
- The Institute will block access to Prohibited Technologies and Covered Applications on all Institute-owned networks to prevent the download, installation, and/or communication of devices to prohibited technologies.

Administrative Controls

Measures that have been or will be taken include, but may not be limited to, the following:

- Issuance of this standard;
- As necessary and based on the level of risk presented to the Institute, removal of content on Institute webpages referencing and/or linking to Prohibited Technologies or Covered Applications other than those used to communicate and facilitate compliance with the orders, such as this standard;
- Development of procurement procedures and review of institutional procurement activities to restrict the acquisition of Prohibited Technologies and Covered Applications;
- Reviews of institutional research activity and grants regarding Prohibited Technologies and Covered Applications and development of procedures to avoid such activities without an authorized exception;
- Development of procedures to identify and remediate Prohibited Technologies or Covered Applications controlled by the Institute and external parties on behalf of the Institute;
- Communication to multiple stakeholder groups;
- Establishment and reporting of exceptions authorized by the Institute president;
- Identification and designation of Sensitive Locations;
- Updates to Institute cybersecurity awareness programs to include information concerning Prohibited Technologies and Covered Applications; and
- Updates to applicable contracts and contract addenda to reflect the prohibitions of this standard and the TSUS Technologies Prohibited by Regulation Policy.

Procedures

Procedures for Personnel

The following general procedures should be followed by Personnel who are aware of the use of a Prohibited Technology, Covered Application, or Unauthorized Device to conduct Institute Business.

1. Stop using the Prohibited Technology, Covered Application, or Unauthorized Device.
2. Report the use of Prohibited Technology, Covered Application, or Unauthorized Device using the Institute's Information Security Incident Form if the technology is:
    - Installed on or accessed from an Institute-owned device,
    - Incorporated as part of a department's or unit's business or otherwise represents the Institute, or
    - A component of the Institute's infrastructure.
3. For personal devices used to conduct Institute Business:
    - Remove the Prohibited Technology or Covered Application, or
    - Cease using the personal device for Institute Business and remove all Institute data from the personal device.

Procedures for Specific Technologies Prohibited by Regulation

Procedures to Disable Social Media Accounts

To mitigate the likelihood of username reclamation and subsequent impersonation by threat actors, the following procedures are to be implemented by the respective information resource owner and information resource custodian of Institute-managed social media accounts:

1. Archive copies of content posted to the account and store the archived copies in an authorized location (e.g., Institute file share or SharePoint) in compliance with the records retention schedule.
2. Remove all content from each account.
3. De-brand each account by removing all institutional logos, contact information, and similar details.
4. Set the account to private.
5. Leave the account active and maintain it under Institute control by storing the credentials in a secure manner.
6. Remove any remaining instances of the application from Institute-owned devices.
7. Confirm the account has been registered with Information Technology Services and do not use it further.

Additional procedures may include temporarily logging on to the account from an authorized source to prevent deactivation of the account and loss of the account's reserved username after a period of inactivity as determined by the relevant social media service (e.g., 170 days for TikTok). These procedures may be activated based on several factors, including risk analysis, shifts in the threat landscape, and the status of authorized exceptions.

Procedures for Exceptions to Technologies Prohibited by Regulation

The following procedures should be followed by personnel seeking an exception.

1. Exceptions may be requested using the Information Security Policy Exception Form.
2. Exceptions must include a detailed business justification.
3. Additional information may be requested to determine if an exception is possible.
4. Exceptions may only be approved by the Institute's president.
5. Approved exceptions will be reported to the Texas Department of Information Resources.
6. Approved exceptions may be subjected to review by the Office of the Governor, the Texas Legislature, or others appointed to review.

If you have any questions regarding this Standard, please review the Technologies Prohibited by Regulation FAQ.

Revision History

This section will be updated when any changes are made to this standard.

Date	Summary of Changes
12/9/2022	First Published
02/10/2025	Updated to align with the expanded requirements from DIR/DPS model plan for Prohibited Technologies and Texas Government Code Section 620 concerning Covered Applications. Updated to align with Governor's proclamation.