29.01.06 Covered Applications and Prohibited Technologies

Approved April 8, 2025
Next Scheduled Review: April 8, 2030

Regulation Summary

This regulation implements Texas Government Code Chapter 620 and the Governor's Directive to State Agency Heads, December 7, 2022 (Governor's Directive"), in respect to protecting the state of Texas from software, applications, hardware, and equipment that pose a risk to the state of Texas if the developer or manufacturer may be required by a foreign government, or an entity associated with the foreign government, to provide confidential or private personal information collected by the software, application, hardware, or equipment to the foreign government or associated entity without substantial due process rights or similar legal protections; or the software, application, hardware, or equipment poses a similar risk to the state's sensitive information and critical infrastructure. Chapter 620 of the Texas Government Code and Governor's Directive require The Texas A&M University System (system) to remove covered applications and prohibited technologies published on the DIR Covered Applications and Prohibited Technologies list from state-owned and state-issued devices, and to block access to prohibited technologies from state-owned networks. This regulation applies to the system and its members, including their employees, contractors, interns, and any users of member-owned networks.

Definitions

Click to view Definitions.

Regulation

1. MANAGING MEMBER-OWNED DEVICES AND NETWORKS

    1.1 Except where approved exceptions apply, members must implement appropriate:

        1.1.1 Administrative controls to identify, track, control, and manage member-owned devices.

        1.1.2 Administrative controls to prohibit the procurement, use or installation of covered applications and prohibited technologies on all member-owned devices, including mobile devices, tablets, desktop and laptop computers, and other internet-capable devices.

1.1.3 Administrative controls to prohibit personal devices with covered applications or prohibited technologies from connecting to member technology infrastructure, specifically local networks and VPN connections. Connections to public-facing information resources through the Internet (such as the member's public website or publicly available applications) are excluded from this prohibition.

1.1.4 Technical controls to prohibit the installation of and access to covered applications and prohibited technologies on member-owned devices.

1.1.5 Technical controls to maintain the ability to remotely wipe non-compliant or compromised member-owned mobile devices.

1.1.6 Technical controls to maintain the ability to remotely uninstall covered applications and prohibited technologies from member-owned devices.

1.1.7 Technical controls to deploy secure baseline configurations for member-owned devices as determined by the member.

1.1.8 Technical controls on all member technology infrastructure(s) to prohibit communication with covered applications and prohibited technologies except where an approved exception exists.

1.2 Members must apply the appropriate administrative and technical controls required in section 1.1 to all covered applications and prohibited technologies listed on DIR's Covered Applications and Prohibited Technologies, including any updates as published by DIR from time to time.

1.3 Members may provide a separate logical or physical network for access to prohibited technologies with the approval of the applicable member's chief executive officer ("CEO").

2. MANAGING PERSONAL DEVICES

2.1 Member employees and contractors are prohibited from installing or operating covered applications and prohibited technologies on any personal devices that are used to conduct state business.

2.2 Members must include the provisions of this regulation that are applicable to individual users in their rules of behavior and require all users of member-owned networks to acknowledge the rules of behavior as part of their annual security awareness training.

3. IDENTIFICATION OF SENSITIVE LOCATIONS

3.1 Information owners will:

3.1.1 Designate approved physical and logical locations (sensitive locations) used to discuss Confidential or Internal Use information of a sensitive nature that must be protected from unauthorized disclosure or public release.

3.1.2 Identify the information under their control that requires protection from unauthorized disclosure which will be only discussed within sensitive locations.

3.2 Members must implement appropriate administrative controls to prohibit devices with covered applications or prohibited technologies from entering sensitive locations, including any electronic meeting designated as a sensitive location when discussions involving sensitive information take place.

3.3 Visitors granted access to sensitive locations are subject to the same limitations as employees and contractors on covered applications and prohibited technologies-enabled devices when entering sensitive locations.

4. EXCEPTIONS

4.1 All exceptions to this regulation are treated as high residual risk decisions as defined in 1 Texas Administrative Code Section 202.75(4)(B) and must be approved by the applicable member's CEO and reported to DIR using established member procedures for processing information security exceptions. This authority may not be delegated.

4.2 Exceptions to covered applications are limited to the following categories:

4.2.1 Providing law enforcement (including but not limited to land management security and safety).

4.2.2 Public safety investigations or other investigations and adjudications required by law, policy or regulation.

4.2.3 Developing or implementing information security measures.

4.3 Exceptions to other prohibited technologies are limited to the following categories:

4.3.1 Providing law enforcement (including but not limited to land management security and safety).

4.3.2 Public safety investigations or other investigations and adjudications required by law, policy or regulation.

4.3.3 Developing or implementing information security measures.

4.3.4 Enforcement of system-owned intellectual property rights.

4.3.5 Research in which a prohibited technology is critical to the project and an approved technology control plan is in place to protect campus research security, data, and networks.

Related Statutes, Policies, or Requirements

Texas Government Code Chapter 620, *Use of Certain Social Media Applications and Services on Governmental Entity Devices Prohibited*

1 Texas Administrative Code Section 202.75, *Managing Security Risks*

Governor's Directive to State Agency Heads, December 7, 2022

DIR Covered Applications and Prohibited Technologies

Statewide Security Plan for Prohibited Technologies

System Policy *29.01, Information Resources*

System Policy Memorandum dated October 7, 2024, titled "The Texas A&M University System's Covered Applications and Prohibited Technology Plan", is superseded by this regulation.

Texas A&M University System Cybersecurity Standards

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

Information Technology
(979) 458-6450