Chapter: Agency Supports and Controls **Title: Prohibited Technologies**	**Effective Date: 2/15/23** Page: 1 of 2 Replaces: Admin. Directive #3 FY23

(a) **Policy.**

Individuals may not install or operate prohibited technologies on any personal device that is used to conduct state business or on any state-issued device.

(b) **Applicability.**

This policy applies to all full- and part-time employees, as well as contractors, paid or unpaid interns, and other users of state networks.

(c) **Definitions.**

(1) **Prohibited Technologies**--any technology provider and any additional hardware or software (e.g., TikTok), as determined by the Department of Information Resources (DIR). The up-to-date list of prohibited technologies is published on the DIR website.

(2) **Sensitive Location**--any location, 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.

(3) **State Business**--accessing 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.

(d) **General Provisions.**

(1) Except where approved exceptions apply, using or downloading prohibited applications or websites is prohibited on all state-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet-capable devices.

(2) Individuals may not install or operate prohibited applications or technologies on any personal device that is used to conduct state business.

(3) Individuals who have a justifiable need to use personal devices to conduct state business may request that their device be enrolled in TJJD's "Bring Your Own Device" program in order to get approval to do so. However, the device and all software related to it may not be listed on the prohibited technologies registry.

(4) Only personal devices (e.g., cell phones, tablets, and laptops) that are enrolled in the "Bring Your Own Device" program may enter or be used to log in to sensitive locations, which includes any electronic meeting labeled as a sensitive location.

(5) Visitors granted access to secure locations are subject to the same prohibitions as contractors and employees on unauthorized personal devices when entering sensitive locations.

(6) If any individual is found to have violated this policy, TJJD may take appropriate action, including terminating its relationship with that individual. An employee found to have violated this policy may be subject to disciplinary action, including termination of employment.

(7) TJJD will implement network-based restrictions to include:

(A) configuring agency firewalls to block access to statewide prohibited services on all agency technology infrastructures, including local networks, WAN, and VPN connections;

(B) prohibiting personal devices with prohibited technologies installed from connecting to agency or state technology infrastructure or state data; and

(C) providing a separate network for access to prohibited technologies with the approval of the executive head of the agency.

(8) TJJD must identify, track, and control state-owned devices (e.g., mobile, desktop, and other internet capable devices) to prohibit the installation of or access to all prohibited applications. TJJD will manage all state-issued mobile devices by implementing security controls, including:

(A) restricting access to “app stores” or non-authorized software repositories to prevent the installation of unauthorized applications;

(B) maintaining the ability to remotely wipe non-compliant or compromised mobile devices;

(C) maintaining the ability to remotely uninstall un-authorized software from mobile devices; and

(D) deploying secure baseline configurations, for mobile devices, as determined by TJJD.

(9) If additional technologies are added to DIR's prohibited technologies list, TJJD will implement the prohibition and removal of those technologies. TJJD may also prohibit technology threats in addition to those identified by DIR and the Department of Public Safety.

(10) Exceptions to the ban on prohibited technologies may be approved only by the executive director. This authority may not be delegated.

(A) Exceptions to this policy will be considered only when the use of prohibited technologies is required for a specific business need, such as enabling criminal or civil investigations or for sharing of information to the public during an emergency.

Note: For personal devices used for state business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period of time. To the extent practicable, exception-based use should only be granted for devices that are not used for other state business and on non-state networks. Cameras and microphones should be disabled on devices for exception-based use.

(B) All approved exceptions to the ban on prohibited technologies must be reported to the DIR.

(11) All employees shall sign a document annually confirming their understanding of this policy.