EXECUTIVE DIRECTIVE

SUBJECT: **PROHIBITED TECHNOLOGIES SECURITY POLICY**

AUTHORITY: Tex. Gov't Code §§ 493.001, 493.006(b); BP-02.08, "Statement of Internal Controls;" Statewide Plan for Preventing Use of Prohibited Technology in State Agencies (Final OOG) (texas.gov)

REFERENCE: TDCJ *Information Resources Security Program*

APPLICABILITY: This policy applies equally to all individuals granted access privileges to any Texas Department of Criminal Justice (TDCJ) information resources. This policy applies to all equipment that is owned or leased by the TDCJ or connected to the TDCJ network.

POLICY:

To provide protection against ongoing and emerging technological threats to the state's sensitive information and critical infrastructure, except where approved exceptions apply, the use or download of prohibited applications or websites is prohibited on all state-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

DEFINITIONS:

The following terms are defined for the purpose of this directive and are not intended to be applicable to other policies or procedures.

"Information Resources" (IR) means the procedures, equipment, or software that are employed, designed, built, operated, or maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

"Sensitive location" is 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.

"Unauthorized Devices" means any device, whether TDCJ or personally owned, that includes any prohibited hardware or software.

"User" is any employee, contract employee, consultant, vendor, intern, or volunteer authorized to access the IR by the information owner, in accordance with the owner's procedures and rules.

PROCEDURES:

I. General Guidelines

A. TDCJ will implement the removal and prohibition of any listed technology.

B. TDCJ may prohibit technology threats in addition to those identified by the Texas Department of Information Resources (DIR) and the Texas Department of Public Safety (DPS).

C. TDCJ will configure agency firewalls to block access to statewide prohibited services on all agency technology infrastructures, including local networks, the TDCJ wide area network (WAN), and virtual private network (VPN) connections.

D. TDCJ will prohibit personal devices with prohibited technologies installed from connecting to agency or state technology infrastructure or state data.

E. TDCJ will provide a separate network for access to prohibited technologies with the approval of the TDCJ executive director.

F. TDCJ will identify, track, and control state-owned devices to prohibit the installation of, or access to, all prohibited applications. This includes the various prohibited applications for mobile, desktop, or other internet capable devices.

G. TDCJ will manage all state-issued mobile devices by implementing the security controls listed below:

1. Restricting access to "app stores" or non-authorized software repositories to prevent the install of unauthorized applications;

2. Maintaining the ability to remotely wipe non-compliant or compromised mobile devices;

3. Maintaining the ability to remotely uninstall un-authorized software from mobile devices; and

4. Deploying secure baseline configurations for mobile devices, as determined by TDCJ.

H. Sensitive locations must be identified, cataloged, and labeled by the agency.

I. Unauthorized devices such as personal cell phones, tablets, or laptops may not enter sensitive locations, which includes any electronic meeting labeled as a sensitive location.

J. Visitors granted access to secure locations are subject to the same limitations as contractors and employees on unauthorized personal devices when entering secure locations.

K. All users shall sign a document annually confirming their understanding of this policy.

II. Exceptions

A. Exceptions to the ban on prohibited technologies may only be approved by the TDCJ executive director. This authority may not be delegated. All approved exceptions to the TikTok prohibition or other statewide prohibited technology must be reported to DIR.

B. Exceptions to the policy will only be considered 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. 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 performed on 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.

III. Enforcement

Violation of this policy may result in disciplinary action in accordance with PD-22, "General Rules of Conduct and Disciplinary Action Guidelines for Employees," which may include termination for employees and temporary employees, a termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of TDCJ IR access privileges, and may be subject to civil and criminal prosecution.

Bryan Collier*
Executive Director

* Signature on File

The following list of prohibited technologies is current as of January 23, 2023. The up-to-date list is published on the DIR website at https://dir.texas.gov/information-security/prohibited-technologies.

Prohibited Software, Applications, and Developers

- TikTok;
- Kaspersky;
- ByteDance Ltd.;
- Tencent Holdings Ltd.;
- Alipay;
- CamScanner;
- QQ Wallet;
- SHAREit;
- VMate;
- WeChat;
- WeChat Pay;
- WPS Office; and
- Any subsidiary or affiliate of an entity listed above.

Prohibited Hardware, Equipment, and Manufacturers

- Huawei Technologies Company;
- ZTE Corporation;
- Hangzhou Hikvision Digital Technology Company;
- Dahua Technology Company;
- SZ DJI Technology Company;
- Hytera Communications Corporation; and
- Any subsidiary or affiliate of an entity list above.