Covered Applications Policy for Governmental Entities

Scope and Definitions

Pursuant to Senate Bill 1893, governmental entities, as defined below, must establish a covered applications policy:

- A department, commission, board, office, or other agency that is in the executive or legislative branch of state government and that was created by the constitution or a statute, including an institution of higher education as defined by Education Code Section 61.003.
- The supreme court, the court of criminal appeals, a court of appeals, a district court, or the Texas Judicial Council or another agency in the judicial branch of state government.
- A political subdivision of this state, including a municipality, county, or special purpose district.

This policy applies to all Post Oak Savannah Groundwater Conservation District (the "District") full- and part-time employees, contractors, paid or unpaid interns ("District employees") and other users of government networks. All District employees are responsible for complying with this policy.

A "Covered Application" is:

- The social media service TikTok or any successor application or service developed or provided by ByteDance Limited, or an entity owned by ByteDance Limited.
- A social media application or service specified by proclamation of the governor under Government Code Section 620.005.

Covered Applications on Government-Owned or Leased Devices

Except where approved exceptions apply, the use or installation of Covered Applications are prohibited on all government-owned or -leased devices, including cell phones, tablets, desktop and laptop computers, and other internet-capable devices.

The District will 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 a Covered Application.
b. Prohibit the use of a Covered Application.
c. Remove a Covered Application from a government-owned or -leased device that was on the device prior to the passage of S.B. 1893 (88th Leg, R.S.).
d. Remove an application from a government-owned or -leased device if the Governor issues a proclamation identifying it as a Covered Application.

The District will manage all government-owned or reimbursed mobile devices by implementing the security measures listed below to the extent able:

a. Inform all personnel that all mobile devices used for governmental business are prohibited from the installation of unauthorized or Covered Applications. All applications for such mobile devices must be evaluated and approved by the Information Security Officer (District General Manager/Personnel Director/IT Director) or other designated Information Security Officer prior to purchase and/or installation.

Ongoing and Emerging Technology Threats

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.

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 items on this list as Covered Applications that are subject to this policy.

If the Governor identifies an item on the DIR-posted list described by this section, then the District will remove and prohibit the Covered Application.

The District may also prohibit applications or services in addition to those specified by proclamation of the Governor. The District's Information Security Officer has the authority to require removal and prohibit use of any application, service, or program for District business which he/she determines is a threat to the Confidentiality, Integrity, or Availability of any District system or database.

Bring Your Own Device Policy

To the extent the District has implemented a "Bring Your Own Device" (BYOD) program, the District may prohibit the installation or operation of covered applications on employee-owned devices that are used to conduct government business.

Covered Application Exceptions

The District's Information Security Officer may permit exceptions authorizing the installation and use of a covered application on government-owned, leased devices or reimbursed devices consistent with the authority provided by Government Code Chapter 620.

Government Code Section 620.004 only allows the District to install and use a covered application on an applicable device to the extent necessary for:

(1) Providing law enforcement; or
(2) Developing or implementing information security measures.

If the District's designated Information Security Officer authorizes an exception allowing for the installation and use of a covered application, the District must use measures to mitigate the risks posed to the District and other governmental entities during the application's use including:

- Exclusion of the device from protected networks;
- Monitoring of application use by the District's designated Information Security Officer; and/or
- Revocation of the exception if a violation of any information security measure required by the District's Information Security Officer occurs.

The District must document whichever measures it took to mitigate the risks posed to the District or other governmental entities during the use of the covered application.

Policy Compliance

The District will verify compliance with this policy through various methods, including but not limited to, IT/security system reports, information security officer audits, random review of devices and feedback to leadership. The District reserves the right to review all District-issued devices as well as District reimbursed devices or devices used for governmental business.

An employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment including acceleration of the District's disciplinary and escalation procedures.

Policy Review

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