CITY OF DENTON

Policy Number and Title:	506.12 Covered Applications Policy
Policy Section and Chapter:	Technology Services
Policy Owner & Contact:	Technology Services – Chief Technology Officer
Policy or Directive:	Policy
Last Revision Date:	10/18/2024

POLICY PURPOSE STATEMENT

Pursuant to Senate Bill 1893 (88th Legislature, Regular Session) governmental entities, including the City of Denton as a political subdivision, must establish a Covered Applications policy prohibiting the use of certain social media applications and services on devices owned or leased by the City if those applications or services are identified in the statute or by proclamation of the Governor of the State of Texas upon recommendation by the Department of Information Resources to address vulnerabilities presented by the use of such applications or services.

This policy applies to all City of Denton full- and part-time employees, contractors, paid or unpaid interns, and other users of devices owned or leased by the City of Denton. All City of Denton employees are responsible for complying with this policy.

POLICY

I. Covered Applications

A. The use or installation of Covered Applications is prohibited on all devices owned or leased by the City of Denton (the City) including cell phones, tablets, desktop and laptop computers, and other internet-capable devices.

B. The City will identify, track, and manage all City-owned or -leased devices including phones, tablets, laptops, desktop computers, or any other internet-capable devices to:

1. Prohibit the installation of a Covered Application.
2. Prohibit the use of a Covered Application.
3. Remove a Covered Application, including Covered Applications on the device prior to the implementation of this Policy.
4. Remove an application at any time if it is identified as a Covered Application.

C. The City will additionally manage all City-owned or leased mobile devices by implementing the security measures listed below:

1. Restrict access to “app stores” or unauthorized software repositories to prevent the installation of Covered Applications.
2. Maintain the ability to remotely wipe non-compliant or compromised mobile devices.
3. Maintain the ability to remotely uninstall unauthorized software from mobile devices.

D. The Director of Technical Services or designee shall ensure timely compliance with the requirements of Texas Government Code Chapter 620 and the related Texas Governor's proclamations regarding Covered Applications or Services and shall review the published lists of the Department of Information Resources and Department of Public Safety to ensure the department stays apprised of the list of the Covered Applications and Services.

II. Ongoing and Emerging Technology; Policy Review

A. To provide protection against ongoing and emerging technological threats to the City's sensitive information and critical infrastructure, Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) regularly monitors and evaluates additional social media applications or services that pose a risk to this state.

B. DIR will annually submit to the Governor of the State of Texas 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.

C. If the Governor identifies an item on the DIR-posted list described by this section, the City will remove and prohibit the Covered Application from all City-owned or -leased devices.

D. The City may also prohibit social media applications or services in addition to those specified by proclamation of the Governor.

E. The Technology Services Department will review the list of Covered Applications at least annually.

III. Covered Applications Expectations

A. The installation and use of Covered Applications on City-owned or -leased devices is permitted only to the extent necessary for:

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

B. The City will use the following measures to mitigate the risks posed to the City or state from the installation or during the application's use:

1. An exception to install a Covered Application must be approved by the City Manager.
2. The Director of the Department will ensure the number of users will be limited to only the number of people necessary for the effective use of the Covered Application for the purpose stated in the request for approval by the City Manager.
3. The Technology Services Department will report any known cyber event related to a Covered Application to the City Manager.
4. The Technology Services Department will advise any departments receiving approval by the City Manager on the implementation of best practices to mitigate risk from installation or use from the Covered Application.

C. The Director of the Department will document the measures taken to mitigate the risks posed to the City or state from the use during the use of the covered application.

ROLES AND RESPONSIBILITIES

I. DPS (Texas Department of Public Safety)

The State of Texas agency designated to regularly monitor and evaluate public safety security risks related to covered applications.

II. DIR (Department of Information Resources)

State of Texas agency that works with DPS and Texas Governor's office to provide updated information on additional social media applications and services identified as posing a risk to Texas.

III. CISO (Chief Information Security Officer)

State of Texas official that keeps up to date tracking of all current covered applications proclaimed by the Texas State Governor.

IV. Technology Services

Responsible for maintaining all City of Denton-owned or leased mobile devices to assure they do not have covered applications installed.

V. The Director of Technical Services or designee

a. Responsible for keeping a current list of "Covered Applications" and ensuring employees are informed of the Covered Applications list and additions or changes to the list.

ADMINISTRATIVE PROCEDURES

Available within the Technology Services Department

DEFINITIONS

Covered Applications - A social media application or service specified by proclamation of the Governor of the State of Texas under Government Code Section 620.005.

REFERENCES

- Government Code Ch. 620, including specifically Section 620.005
- Senate Bill 1893

REVISION HISTORY

Revision Date	Policy Owner	Summary
09/23/2024	L. Meine (TS)	• Initial Policy implementation
10/18/2024	L. Meine (TS)	• Policy updated to meet Government code 620.005
09/30/2024	l. Meine (TS)	• Updated policy to reflect living changes from Government Code 620.005 • Establish the creation of an SOP for Covered Applications management.