Chapter: Conditions of Employment **Effective Date: mm/dd/yyyy**
Policy: Prohibited Technology on City Devices

New

Policy.

In compliance with Chapter 620, Texas Government Code, the City of Crockett (City) prohibits the use or installation of covered applications as defined in this policy on all City-owned or City-leased devices, including cell phones, tablets, desktop and laptop computers, and other internet-capable devices used by any employee, contractor, volunteer, library patron, or any other user except to the extent necessary for providing law enforcement or developing or implementing information security measures. Any person who possesses or uses a City-owned or City-leased device must ensure that any covered application that was installed on the device prior to the effective date of this policy is immediately removed.

The intent of the limitations in this policy is to protect against ongoing and emerging technological threats to sensitive information and critical infrastructure.

The City does not intend to restrict an employee's use of a covered application on any device that is not owned or leased by the City.

Additional Resources.

- City of Crockett Social Media Policy (published on the City's website for persons accessing and posting on the City's social media sites).
- PD-2.10, Personal Use of Social Media

Definition.

"Covered Application" means the social media service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited or a social media application or service specified by proclamation of the governor as posing a risk to the State of Texas

"Social Media" means publicly available, internet-based platforms that publish user-generated content. This includes blogs and microblogs (e.g., Pinterest, Twitter, The Daily Beast), wikis, media-sharing sites (e.g., Instagram, YouTube, SlideShare), podcasts, social networking sites (e.g., Facebook, Myspace, LinkedIn), mash-ups, virtual worlds (e.g., gaming programs and sites), and similar application or technologies currently in existence or other platforms that may be developed in the future.

Procedures.

I. Monitoring and Managing City-Owned or City-Leased Devices.

A. The City will identify, track, and manage all City-owned or City-leased devices including mobile 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 from a City-owned or City-leased device that was on the device prior to the effective date of this policy; and

4. Remove an application from a City-owned or City-leased device if the Governor issues a proclamation identifying it as a covered application.

B. In addition to a covered application, the City may prohibit other technology threats on City-owned or City-leased devices if the City determines that such prohibition is appropriate.

C. The City may manage all City-owned or leased mobile devices by implementing security measures that include but are not limited to the following:

1. Restricting access to “app stores” or unauthorized software repositories to prevent the installation of unauthorized applications;

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

3. Maintaining the ability to remotely uninstall unauthorized software from mobile devices.

II. Managing Exceptions.

A. Only a City administrator may authorize an exception to the installation or use of a covered application for the purpose of providing law enforcement or developing or implementing information security measures.

B. When an exception is authorized, the City will implement the following measures to mitigate risks during the use of the covered application:

1. The exception will be granted for a predefined period of time.

2. To the extent practicable or possible, the exception-based used will only be performed on devices that are not used for other City business and on non-City

networks, and the user should disable camera and microphones on devices authorized for exception-based use.

C. The City administrator authorizing the exception will document the following:

1. The date, time and reason for the exception;

2. The specific application used, the person(s) using the application, and the device on which the application was used;

3. The specific measures implemented to mitigate risks during the use of the covered application; and

4. The date and time that the covered application was uninstalled from the device after the period of authorized use is complete.

III. Employee Duty to Report Violation of Policy.

Any employee who observes or learns about the installation or use of a covered application on a City-owned or City-leased device must promptly notify his immediate supervisor, administrator, or the City Secretary.