# Exhibit B

## Personnel Policy

Note- New text is shown as red and underlined.

### 2.11 NETWORK AND INTERNET USAGE POLICY AND PROHIBITED TECHNOLOGY APPLICATIONS

The City of Burnet provides Network and Internet Usage for City business when necessary in the performance of the employees' duties. The City is responsible for securing its own network and computing systems in a reasonable and economically feasible degree against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users.

Employees should be aware the City of Burnet's voicemail, e-mail and computer systems are the City of Burnet's property, for the use and benefit of the City of Burnet and that all information stored in these systems is subject to review by management without prior notice to employee and are subject to public inspection under the Texas Public Information Act.

The City Manager will designate a Systems Administrator for all facilities that have access to network or internet usage. To that end, the City has developed the following policy for Network and Internet usage:

- Access – Employee Internet access must be authorized by the System Administrator. A condition of authorization is that all Internet users must agree to this policy as signified by their signature on the acceptance page of this Personnel Policy.
- User password and ID's – Authorized users are assigned a user ID and password upon being given access to the system. User ID's and passwords shall not be changed or altered in any way without express consent of the System Administrator. Protection of the ID and password are the responsibility of the User therefore sharing them with any other person is strictly prohibited. The User can be held responsible for the actions of persons using their ID or password.
- Deletion, examination, copying or modification of files and/or data belonging to other users without their prior consent is prohibited unless specifically authorized by the System Administrator.
- Distribution of information gathered from the system to unauthorized persons is prohibited and the employee is subject to disciplinary action.

- Installation or downloading of hardware or software without the approval of the System Administrator is prohibited and is subject to immediate disciplinary action.
- Employees shall report all computer virus outbreaks to the System Administrator. The System Administrator shall take action reasonably necessary to prevent the spread of a computer virus to other computers.
- Use of facilities for commercial gain is strictly prohibited.
- Use of facilities and/or services for viewing, obtaining, or distributing pornographic materials or other materials not specific to City business is prohibited and will be subject to immediate disciplinary action.
- Any unauthorized, deliberate action, which damages or disrupts any devices on the system including but not limited to viruses or other disruptive/destructive programs, is prohibited and may result in disciplinary action.
- Allowing unauthorized individuals to access system files is prohibited and is subject to disciplinary action.
- Unauthorized use of Electronic Mail is prohibited. This may include sending junk, harassing, obscene or threatening mail; sending solicitations for the purpose of personal financial gain; forgery of electronic signatures; prolonged or excessive use of electronic mail for personal use and/or attempting to read, delete, copy or modify the electronic mail of other users. Any emails of a personal nature should include the following disclaimer “This e-mail contains the thoughts and opinions of the (employee’s name) and does not represent official City policy”. Personal e-mails are to be kept at a minimum and should not be disruptive to daily activities and responsibilities.
- Violation of copyright laws is prohibited.
- Accessing web sites that charge fees for access, software, services or literature is prohibited unless specifically authorized by the System Administrator, Department Director or Finance Officer.
- Online chat is prohibited.
- Installing and/or playing games is prohibited. Playing online games is prohibited.
- Representing yourself as another person is prohibited.

Some guidelines to avoid unintentional violations are:

- Only access sites on the Internet that are related to your job classification.
- Do not download any files without permission from the System Administrator.

- If by mistake you find yourself in an inappropriate or questionable site, close the browser immediately either by clicking on the small X in the upper right corner or by clicking on File and then close. Notify the System Administrator immediately.
- Never open an attachment that you do not expressly know the contents of. Do not open “junk” email or forward chain letters.
- Make sure your virus protector is enabled at all times. Contact your System Administrator if you are not sure.
- Report any questionable activity or responses to the System Administrator immediately.

Prohibited Technology Policy

This policy applies to all City of Burnet employees, contractors, interns, and users of City networks.

In response to Governor Greg Abbott's December 7, 2022, directive and Senate Bill 1893, the City of Burnet has implemented this policy to ban the use of TikTok and other covered applications on City-owned devices to protect sensitive information from potential surveillance threats. The Texas Department of Public Safety (DPS), along with the Texas Department of Information Resources (DIR) provide guidance on managing the provisions of this policy.

This policy allows for the identification, tracking, and management of all City-owned or -leased devices.

This policy governs the use of certain applications, particularly:

- TikTok or any successor developed by ByteDance Limited.
- Applications specified by the Governor under Government Code Section 620.005.

Requirements of the policy include:

- Covered applications cannot be installed or used on City-owned or leased devices, including phones, tablets, and computers.
- The City will manage its devices to:
    - Block the installation of covered applications.
    - Remove any prohibited applications.
    - Implement security measures, including restricting app store access and remotely wiping non-compliant devices.

- City employees must not install or use TikTok or other prohibited applications on any personal devices that are used for City business, including accessing City data, applications, email, VoIP, SMS, video conferencing, and other City databases.

Written exceptions may be granted for:

- Law enforcement activities.
- Developing or implementing security measures.

The City will monitor compliance using IT/security reports. Violations of this policy may result in disciplinary actions, including termination.

This policy will be updated periodically to align with changes in state law, new applications identified under Government Code Section 620.006, and the City's evolving needs.