A. Technology Acceptable Use

1. Policy

The City provides team members with technology resources, consisting of electronic communication systems, a network connection, and Internet/Intranet access in an effort to help team members do their jobs more efficiently. This policy governs all use of the City’s network, Internet/Intranet, electronic communications-related systems, and all associated technology. This policy applies to, but is not limited to computer equipment, telecommunications equipment, printers, software, operating systems, storage media and network accounts providing electronic-mail, Internet, FTP, the City’s Intranet, and all other City electronic messaging and communicating systems, as well as personal devices used to connect to City systems.

2. Purpose

The purpose of this policy is to outline the acceptable use of technology at the City. These guidelines are in place to protect team members and the City. Inappropriate use exposes the City and its users to risks including virus attacks, compromise of network systems and services, fines, criminal and/or civil charges, breech of privacy/confidentiality, potential interruption of services (including emergency and protective services) and liability.

3. Applicability

This policy applies to City team members, elected officials, Committee/Board members, customers, visitors, guests, external contractors/vendors, consultants, personnel affiliated with third parties or anyone else when they are using equipment or systems that are owned or leased by the City, whether during or outside of work hours.
4. General Guidelines

a. Use of the network, associated systems, and Internet/Intranet access may extend throughout a team member’s term of employment. Any person not actively under the City's employ or assign does not have permission to access or use any City system or device unless said device is specifically designed for “public” or “guest” use by the Information Technology Department.

b. The City’s communication systems, network, and Internet/Intranet access are intended for business use only. The City does allow incidental, non-disruptive, casual personal use at the sole discretion of supervisors or managers. Such use is allowed providing it does not interfere with the performance of duties and/or the business use of these systems and is in compliance with all other terms of this and all other City policies.

c. **If there is any uncertainty regarding permissible personal use, it is the responsibility of the team member to consult his or her supervisor for clarification before proceeding.**

d. All information created, transmitted, or received via the City’s communication systems, including but not limited to, e-mail, network, or Internet/Intranet is the property of the City. Team members should have no expectation of privacy regarding this information. The City reserves the right to (and on occasion does) access, read, review, monitor, and copy all messages and files on its computer systems at any time and without notice to the relevant team member(s). The Information Technology Department may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring team members are using the systems consistent with this policy.

e. Any content created or transmitted via these systems constitutes a public record and therefore may be subject to public disclosure in accordance with state law. The City reserves the right to disclose any electronic records or data to law enforcement agencies, the media, or other third parties without the team member’s consent.
f. Any team member aware of a policy violation should immediately report the violation to his/her supervisor, the Director of Information Technology, or the Director of Human Resources.

g. All team members are required to follow the City’s Records Retention and Management policies when considering removing any files that no longer have a practical use.

5. Prohibited Technologies on City-Owned Devices

In compliance with S.B. 1893 and to ensure protection of the City’s sensitive information and critical infrastructure, the City of New Braunfels will maintain a “Prohibited Technologies” list, attached as Addendum A to this policy. This list is compiled and maintained by the Texas Department of Information Resources (DIR) with input from Texas DPS and others. The City of New Braunfels may add additional items to the list, as well as update this list based on new entries at the State/Federal level. Any items on this list shall be prohibited for installation/use on all City-owned and City-issued devices capable of internet connectivity. Prohibited technologies may also be blocked at the network level by the City, thus preventing access over the network, including the “Guest” Wi-Fi network. Violations of this policy may result in disciplinary action up to termination. Exceptions may be made under special circumstances but must be approved by a member of the City Manager’s Office. To the extent practicable, exception-based use should only be performed on devices that are not used for other city business and on non-city networks.

B. Network Access

1. Responsibilities

It is the responsibility of the Information Technology Department to create, manage, and support all user accounts. Each team member is assigned a unique Network ID (user account) and password. This information is used when accessing any electronic and communication systems.
2. **Policy**

By accepting an account and accessing the City’s network, Internet/Intranet, or other communication systems, all City team members agree to adhere to the City policies regarding their use.

a. Each team member is responsible for all actions performed by his or her user account. Therefore, team members shall not disclose their account information.

   1. An exception can be made at the team member’s discretion to provide account information to Information Technology Department staff for support purposes.

b. A team member may at any time request that his or her password be changed.

c. Any team member who has knowledge of someone else’s password should notify that person immediately so he or she can request a password reset.

d. Only under unique circumstances will more than one person utilize the same username and password.

   1. This request must be made by the Department Director and approved by the Director of Information Technology.

3. **Confidential Information**

1. Team members may have access to confidential information about the City, other team members, customers, or citizens. Within the bounds of assigned job duties, team members may use electronic communications to transmit confidential information internally to other team members with a legitimate need to know. For the purpose of this policy, confidential information includes, but is not limited to:

   a. Procedures for computer access and User IDs to the City’s network or vendors’ systems; program/user manuals, systems flowcharts; all documentation normally related to the design or implementation of any system developed by the City relating to computer programs or systems installed for customers,
citizens or internal use.

b. Team member financial information, Social Security numbers, health records, personal health information (PHI) and other confidential material.

c. Lists of present team members, clients and customers and the names of individuals with whom the City deals, the type of equipment or computer software they use, and information relating to those clients and customers, which has been given to the City by them or developed by the City relating to computer programs or software installed.

d. Lists of, or information about, persons seeking employment with or who are employed by the City.

e. Any other information relating to the City’s network, infrastructure, and engineering.

4. New Team Members

1. Upon hiring a new team member to fill a previously filled position, it is the responsibility of the hiring department to complete the IT New Hire Worksheet requesting network access. Upon receiving all necessary forms, IT will setup and configure all accounts and access within one week.

2. When hiring a new position, it is the responsibility of the hiring department to coordinate with the Information Technology Director on filling the position so there is sufficient time to purchase, configure, and install all necessary hardware and software prior to the team member start date.

5. Password Guidelines

Passwords are the key to security. It is important that team members not disclose their password to others. Following are a list of guidelines to help create strong passwords and to help keep those passwords secure:
CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): TECHNOLOGY ACCEPTABLE USE & MOBILE DEVICE

EFFECTIVE DATE: MAY 20, 2019
REVISION DATE(S): OCTOBER 1, 2022, OCTOBER 24, 2023

a. Passwords should not be recorded where they might be easily obtained.
b. Passwords should:
   1. contain no less than eight (8) characters
   2. contain both upper and lowercase characters (e.g. a-z, A-Z)
   3. have at least 2 digits or punctuation characters as well as letters
      (e.g. 0-9,!@#$%^&*()_+-=|{}~?><)
   4. not be a word found in the dictionary

6. Terminations

   Immediately upon separation of employment, the IT Department will disable all user
   account(s) and network access. Arrangements should be made with the Director of
   Information Technology prior to separation of employment to provide alternate access to
   the team member’s email information and files. Once the vacant position has been filled,
   the IT Department will archive all user data according to the Records Retention and
   Management Policy.

7. Data Storage & Backups

   All important, confidential or proprietary information should be stored on the network. The
   network is equipped with electronic and physical security. Activity on the network is
   monitored for tampering and other security breaches. The Information Technology
   Department is responsible for backing up data and programs that are on the network.

C. Software

1. Downloading & Installing
In an effort to maintain a secure, standardized environment and to prevent violating software licenses, team members shall not download or install any software on their computers unless prior approval has been given by the IT Department. The IT Department is responsible for the installation, maintenance, and support of all software and updates on all information technology systems, except where other arrangements have been made.

2. Licensing & Piracy

Team members are to use software strictly and exclusively in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software is a violation of copyright law. In addition to being in violation of the law, unauthorized duplication of software is contrary to the City’s standards of team member conduct. The City licenses the use of computer software from a variety of outside companies. The City does not own the copyright to software licensed from other companies. Team members acknowledge they do not own software or its related documentation. Team members may not make additional copies of software. The only exception will be a single copy, by Information Technology Department for backup or archival purposes.

a. Under no circumstances are team members permitted to install personal software on the City’s computer system.

b. Team members are not permitted to copy software from the City’s computer system.

c. Team members are prohibited from giving software to persons not employed by the City.

d. Under no circumstances will the City use software from an unauthorized source, including, but not limited to the Internet, home, friends, and/or colleagues.

D. Electronic Communications

1. Purpose
The City's electronic communications systems are designed to improve service to our customers and citizens, enhance internal communications, reduce service provision costs and reduce general paperwork.

2. **Appropriate Use**

Team members using the City's e-mail, voicemail, and all associated systems should adhere to the following guidelines:

   a. Alternate Internet Service Provider or Virtual Private Network (VPN) connections to the City's internal network are not permitted unless expressly authorized by the Director of Information Technology.

   b. Only authorized personnel are permitted to access another person’s e-mail or voicemail without the user’s consent. Such access will only be granted by the Director of Information Technology with the permission of the Department Director.

   c. All electronic communications must conform to City anti-harassment, workplace violence and discrimination policies.

   d. Team members must abide by copyright laws, ethical rules, and other applicable City policies or laws.

3. **Inappropriate Use**

   a. All communications originating from or transmitted via the City's communication system must contain professional and appropriate language at all times. Team members are prohibited from transmitting abusive, harassing, intimidating, threatening and discriminatory or otherwise offensive messages via e-mail, telecommunications, or paging.
b. Use of the City’s electronic communications systems to solicit for any purpose, personal or otherwise, without the consent of the City Manager is strictly prohibited.

c. Sending, forwarding, or hosting unsolicited e-mail messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (e-mail SPAM) is prohibited.

E. Telephone Utilization

1. Purpose

The use of both landline and cellular telephones is necessary to the orderly conduct of business by the City. The purpose of this policy is to enumerate the guidelines for use of telephones by City team members.

2. Acceptable Use

The City’s telephones are to be used for conducting necessary business. The City will acquire, assign and pay the monthly charges on cellular telephones for those team members that require this tool to conduct business for the City. Designated team members may be approved for a cell phone allowance. Limited personal use of City telephones is permitted in accordance with this policy.


a. City telephones, both landlines and cellular telephones, are to be used primarily for conducting necessary City business. Personal telephone calls by a team member are permitted; however, use to the point of interference with performance of job duties may result in corrective action.
PROCEDURE(S): TECHNOLOGY ACCEPTABLE USE & MOBILE DEVICE

EFFECTIVE DATE: MAY 20, 2019
REVISION DATE(S): OCTOBER 1, 2022, OCTOBER 24, 2023

b. Long distance calls for official City business should be made only by personnel authorized by their respective Supervisor to make such calls.

c. Personal long-distance calls should be charged to a personal calling card or be made on a pre-paid phone card. Team members are required to report and reimburse the City for any personal long-distance calls made on City telephones and charged to the City.

d. The City shall pay the monthly charges for City cellular telephones assigned to City team members for use in conducting City business. Team members shall be required to reimburse the City for any additional charges, i.e. additional minute charges, incurred on the cellular phone unless the team member can substantiate that the additional charges were City-related and that the allocated monthly minutes under the provider plan was substantially incurred for City-related business. Excessive personal use of City cellular telephones may result in corrective action.

e. In accordance with City Ordinance 2015-41, team members shall not use a cellular telephone or other hand-held communications device while operating a motor vehicle (emergency vehicles are an exception to this policy). Team members shall pull over and stop before operating a hand-held device. Team members shall not send or read text messages on a hand-held device while operating a motor vehicle.

f. The City’s voicemail system is for improved customer service. Team members shall use the system appropriately keeping in mind that effective communication via telephone is an integral part of establishing and maintaining quality customer service.

F. Wireless Communication

The City of New Braunfels policy is to provide access to a wireless communication device to a City team member when and if the Department Director determines the use of the device is required
and necessary for the performance of the team member’s job duties. The Department Director will determine each year the appropriate device and allowance for the team member. A wireless communication device allowance may be withdrawn by the department at any time.

1. Eligibility

In general, team members will be required to have a wireless communication device that is compatible with the City’s network and E-Mail system if job duties or operational requirements:

a. Involve frequent travel or will routinely take the team member into the field to conduct business but have a need to remain in communication with others for City business purposes.

b. Present a need for constant and immediate communications through the day if the position requires the team member to be away from the office or their desk frequently.

c. Presents a need after hours for a team member that significantly supports or is responsible for programs, services, or systems.

d. Require a team member to be available for emergency or business-related contact on a 24/7 basis.

e. Deem there are no other practical alternatives for cost effective and timely communications using landlines or other communications methods.

f. Simple convenience may not serve as a criterion for requiring a team member to possess a wireless communication device that is compatible with City software.

g. Additionally, supervisors must ensure that requirements for hourly team members to check E-mail, or be available after normal working hours, are clearly understood
and explained to team members, and that such requirements are in accordance with the Fair Labor Standards Act.

2. Security

The City reserves the right to load City supplied software on the device. The software will assist in maintaining network and data security and integrity, including, but not limited to, antivirus and device management products. The software may restrict access to sensitive or confidential information from the device, manage City data on a device used for both City and personal use, or delete or remove City data from the device. The City is not responsible for any decrease in functionality or damage to the device that may result from the use of these software products.

3. Notification Requirements

The team member is responsible for immediately notifying the IT Department and their direct supervisor should their equipment become lost, stolen, or otherwise inoperable. Department Directors must immediately notify both the IT Department and the Human Resources department should a team member under this policy separate from City employment.

**MOBILE DEVICE USE**

[Mobile Device Use Form]

**POLICY**

This policy outlines the usage of mobile devices by team members when used for City business. This policy applies regardless of the location of the worksite. Mobile devices include, but are not limited to, technologies such as cellular telephones, phones, iPads, non-windows tablets, phone tablets (phablets)
or other devices that can digitally access or download email, data files, text files, or Internet sites. City-owned devices including, but not limited to, Apple products, Windows-based tablets (Surface) and laptops do not apply to this policy.

1. Work-related information and data generated on, processed by and/or retained on mobile devices that access City e-mail or other network services, are the property of the City of New Braunfels. Team members that use a mobile device to access City data, or utilize any type of City data, may be required to disclose that information to a member of the public, including the press, pursuant to the Texas Public Information Act.

2. A team member in a position designated as non-exempt under the FLSA will not use a mobile device for City work outside of the team member’s normal work schedule unless the team member receives prior supervisory approval for the specific work performed. In accordance with the City’s policy on Overtime Compensation and Compensatory Time, the team member is only allowed to work overtime or accrue compensatory time with the express permission of the supervisor. The team member must accurately record all time worked within the pay week in which it was worked.

3. Claims for injuries sustained while utilizing mobile devices for work purposes must be reported to the team member’s supervisor pursuant to the City’s Workers Compensation Policy.

4. Any mobile device that accesses City data systems must conform to security access requirements as defined by Information Technology to ensure that the City’s data on the device is protected from unauthorized access and use. Requirements include, but are not limited to, utilization of a password to lock the device and adherence to centrally managed security policies. By utilizing the mobile device for City business, the team member acknowledges that these centrally managed security policies may impact the settings on the device. Access to the City email system will be terminated for any personal mobile device failing to conform to these requirements.
1. Team members may request to their supervisor or Department Director to review a city-owned mobile device for business use while employed with the city. In general, team members will be provided a mobile device if job duties or operational requirements:
   a. Involve frequent travel or will routinely take the team member into the field to conduct business, but have a need to remain in communication with others for City business purposes;
   b. Present a need for constant and immediate communications through the day if the position requires the team member to be away from the office or their desk frequently.
   c. Presents a need after hours for an team member that significantly supports or is responsible for programs, services, or systems;
   d. Require an team member to be available for emergency or business-related contact on a 24/7 basis;
   e. Provide operational efficiencies for remote access to owned or subscribed to software systems;
   f. Deem there are no other practical alternatives for cost effective and timely communications using landlines or other communications methods;

   Simple convenience may not serve as a criteria for requiring an team member to possess a mobile device.

**STIPEND-BASED MOBILE DEVICES**

1. Team members may request to their supervisor and Department Director and receive approval from the City Manager or designee to receive a monthly mobile communication device allowance in lieu of a City owned device.
   
   a. Team members who receive approval for a mobile device allowance are responsible for selecting and contracting with a service provider in their own name for approved
PERSONAL MOBILE DEVICE

1. Personal devices may be used by team members to access City email, calendars, contact information and other approved City data as available per device technology and licensing provisions. However, access is subject to City restrictions, approvals and security controls defined by the Information Technology (IT) department. Failure to adhere to access rules may result in termination of access and/or disciplinary action.

   a. Team member’s Department Director or designee will review each request for personal

   voice/data service or voice only service.

   b. They City will pay the cost of providing the same required level of service per month as if the team member was on a city-owned service plan. This amount will be assessed on an annual basis and is subject to change from year to year. The allowance is not intended to cover the total cost of the fees and service charges incurred under an individual plan. Any charges by the team member’s service provider in excess of the allowance are the personal responsibility of the team member and not the City.

      i. The City Manager or designee may authorize a higher stipend amount as appropriate at his/her discretion

   c. The taxable allowance will be processed through the payroll system and paid to the team member. The allowance is supplemental income and considered taxable income to the team member. The taxable allowance will be subject to required deductions such as FICA and TMRS. The monthly allowance will not constitute an increase in base pay and will not be included in any percentage calculations for an increase to base pay.

   d. To be eligible to receive this allowance, team members must purchase a wireless communication device and plan that is appropriate for their determined use (voice only or voice and data) and is compatible with the City’s network and E-mail system as appropriate.
device use for business purposes, and may approve or deny the request at his or her sole discretion.

b. Utilization of personal mobile devices to access City data in the performance of City work is not mandatory, and is a voluntary election by the team member. The City bears no responsibility for the reimbursement of costs associated with the activity.

2. The cost of making changes to, or the cancellation of, any personal mobile device contract for service, as well as device repairs of any type, is the sole responsibility of the device owner.

   a. The costs associated with utilizing the personal mobile device for City business are the sole responsibility of the device owner. Content that is accessed, displayed, and/or transmitted while using the device for City business must follow City policies in terms of acceptable content in the workplace.

3. Non-exempt team members must also receive approval from their Department Director or designee for how they will utilize their personal mobile device during regular work hours and may not use their personal device to access the City system outside of their normal work hours without prior approval of their supervisor.

4. Basic information on how to configure and access available City services will be available from the Information Technology department. Information Technology is not responsible for ensuring connectivity to City email or other services with personal mobile devices.

5. As part of configuring the device to access City resources, team members must have personal mobile devices configured with an access password to prevent unauthorized use. The City’s IT Department will configure and enforce a forced access password, if one is not already configured.

6. Information Technology will not allow connections from a personal mobile device to City data without a signed acknowledgement form from the team member with appropriate supervisory signatures.
RESPONSIBILITIES

1. Except in certain narrowly defined circumstances, the Texas Public Information Act provides the public the right to access much of the information that governmental bodies produce. The Public Information Act does not differentiate where the data is stored, what format the data is in, or ownership of the device on which data is stored.
   
   a. Personal data on a personal device that is not subject to the Public Information Act requires the City to comply with State and Federal confidentiality laws, as applicable. In order for the City to comply with these requirements and allow public and confidential data to reside on a personal mobile device, users of these devices must follow security guidelines.

   b. It is recommended that only City email, contacts and calendars be accessed from personal devices. Downloading City documents to personal devices is discouraged. Texts are also subject to the Public Information Act.

   c. Security requirements must be followed for all personal mobile devices that contain any type of City data. By using their personal mobile device to access City data, team members acknowledge that their personal mobile devices may come under the review of an audit or Public Information request.

2. Team members are expected to cooperate and assist in obtaining City data from their mobile device, including, but not limited to, temporarily transferring possession of the mobile device to authorized City representatives retrieving City data. Team members will take every reasonable step to preserve the City data on their mobile device until such time that the City data is captured.

3. All approved mobile devices will be connected to technology that will require a device access code and allow for the device to be remotely wiped.
4. City-owned mobile devices may not be used for viewing excessive streaming video including but not limited to Netflix and Hulu.

5. The owner of the personal device must report lost and/or stolen personal mobile devices connected to City data to IT immediately. Any device will be ‘wiped’ when Information Technology is notified of it being lost or stolen. This means that all data on the phone will be erased, including personal data. Upon termination of employment, all data connections will be disabled.

6. Each mobile device user is responsible for ensuring that their device is kept safe, backed up and secure to reduce the likelihood of being lost or stolen.

7. Non-business use of personal mobile devices must not disrupt or interfere with the team member’s or the team member’s co-worker’s workplace duties.

8. The City may periodically change access methods and information systems which may result in incompatibility with personal mobile devices. The personal mobile device owner is solely responsible for ensuring that their device is properly configured and compatible with the services offered by the City.

9. It is the supervisor’s responsibility to maintain a copy of their team member’s authorizations to use personal mobile devices to access City data services.

10. A copy of signed team member authorization forms should be filed in HR and a copy sent to IT and the team member’s department.

Addendum A – Prohibited Technologies

The up-to-date list of prohibited technologies is published at https://dir.texas.gov/information-security/prohibited-technologies. The following list is current as of January 23, 2023:
Prohibited Software/Applications/Developers

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