# GILLESPIE COUNTY

## STATE OF TEXAS

---

# Technology Usage Policy
# Revision 1.5

---

# 2 Table of Contents

# 3 Introduction

The policies and procedures set forth in this manual provide guidelines for management of employees during employment, but do not create contractual rights regarding termination or otherwise. This document is used as a guideline to create base policies for any person that will be connected to, accessing, storing data on, transmitting any other data across, or otherwise using the computer network owned and operated by Gillespie County for any purpose ("User"). The purpose of this Policy is to provide the County, its officials, department heads, agents, contractors, and employees the basis for acceptable use of the County's technology resources. This policy **DOES NOT** replace or supersede any other policy currently in effect as found in the "*Gillespie County Employee Handbook".*

This policy has been reviewed and approved by the Commissioners Court of Gillespie County. All authority granted to the parties named within was vested in the open meeting of the Gillespie County Commissioner's Court on: _October 28th 2024_

To maximize the benefits of the Information Technology investments across Gillespie County, the Information Technology department ("IT") has created this Technology Usage Policy to address and communicate existing and new policies. Goals of this policy are:

1. Support the overall Vision and Goals of Information Technology.
2. Protect confidential, proprietary information of the County from theft or unauthorized disclosure to third parties.
3. Be cost-effective and prevent waste of Information Technology resources.
4. Reduce, and if possible, eliminate, potential legal liability to employees and third parties.

This policy requires that all new and existing County employees sign a written statement acknowledging that they have read and understand this Policy. New employees shall return the written signed statement to Human Resources. Existing employees shall return the written signed statement to Human Resources through their department head or elected official.

## 3.1 Information Technology Vision Statement

Provide value-added technical services and solutions to Gillespie County that enhance or enable better service to its citizens and employees.

## 3.2 Goals

- Ensure the availability and security of our network
- Enable ease of obtaining and sharing of data.
- Lower costs - Achieve IT Standardization where feasible
- Better enable disaster recovery of critical systems.

## 3.3 Guiding Principles:

- IT will provide quality customer service and solutions.
- IT will demonstrate professionalism and be customer focused – to our citizens, County teammates, and business partners.
- IT will maximize our information technology investment by fully leveraging our solutions and services across the County.
- IT will promote and implement standard technology and solutions, where feasible, throughout all County offices to support common business processes.
- IT will use commercially available software packages wherever possible.
- IT will dynamically re-engineer our business processes around the functionality of available application packages.

- IT will work efficiently using best practices.

# 4 Communication

IT will update this policy, as needed, and once approved by the Commissioners Court, will communicate the updates to all Elected Officials, Department Heads and IT Contacts, as appropriate. IT will also provide access to this policy on the County Employee Portal. The County will make reasonable efforts to notify Users when software patches or other software is deployed to User PCs and where there may be a disruption to the User. There will be times where software will need to be deployed where prior notice may not be feasible, as in the case where there is a **security risk or legal/statutory compliance requirement** or where such deployment is transparent to the User, as in the case of operating system or application upgrades; asset inventory data collection, data collection for license management and compliance, or for new software that the county deploys and which can occur in the background without disruption to the User.

# 5 Standards

IT has the responsibility for support and problem resolution for the County's PCs and network. To effectively and efficiently carry out that role, IT must be able to rely on standard hardware and software configurations on the desktop. Users must request hardware and software through Information Technology Services.

## 5.1 Hardware Standards

Department Heads who have a need to deviate from the standards must request an exception. The IT Director will review the request and either approve request as is, or suggest alternate solutions to ensure support can be provided. If a satisfactory solution cannot be agreed upon, the issue will be raised to the appropriate Court Liaison of the Gillespie County Commissioner's Court.

IT is responsible for the configuration and acquisition of ***ALL*** County-owned technology equipment that will interface with the County computer network at any level, or connected to any computer or device that is connected to the County computer network, regardless of what fund pays for said equipment. **Any County-owned technology equipment that is purchased without prior IT approval SHALL NOT be allowed to be connected to ANY County-owned computer or computer network.** It is also the responsibility of the IT department to maintain a current inventory of ***ALL*** County-owned computer equipment owned by Gillespie County and connected to the County's computer network. IT shall have uninhibited access to any County-owned computer equipment that is connected to the County computer network, for inspection and inventory control, upon request at any time.

Due to security configurations of the County network, no County official, department head, employee, or contractor may move or authorize to be moved any County-owned computer equipment that is connected to the County computer network without prior notice to IT. Upon notice, IT shall either move the equipment, approve a User to move said equipment, or disapprove a User to move said equipment. If a User moves any equipment, and does not provide prior notice to IT, the equipment may not function at its new location due to network configurations.

## 5.2 Software Standards

IT must first acquire and test programs and executables before employees download, install, or save the software on their County desktop or computer equipment. Software may only be used in compliance with the terms of the applicable license agreements.

These Software Standards specify the technologies supported by the County and serves as a guideline for all technology purchasing and use decisions, including hardware, software, peripherals, and network components.

### 5.3 Unauthorized Software

Use of unauthorized software can degrade the County's network and Internet service, create security risks and computer problems, divert focus from County-related issues, reduce employee productivity, and increase costs. It is the responsibility of all Users in all departments to comply with maintaining the County standard by not downloading or installing unauthorized software onto any County owned computer. Any software which needs to be downloaded and installed must be performed by IT. **Unauthorized software is defined as any software that is not approved for use by IT to conduct the business of Gillespie County.**

IT will 1) immediately inform the department head, and if warranted, remove the unauthorized software in use when encountered; and 2) on a routine basis, check and remove unauthorized software, unless the software has a legitimate business purpose for the User as determined by IT and the appropriate Department Head.

## 6 Network Resource Usage – Internet, Email & Data

Access to and use of the County's computer network, Internet and/or e-mail systems is provided to employees of Gillespie County for the purpose of advancing the goals and business of the County. This access imposes certain responsibilities and obligations on County employees (including full-time, part-time, and temporary employees), officials, and as well as any companies or individuals (third parties) contracted to do work for the County or use County IT resources. Use of County IT resources is subject to County policies and local, state, and federal laws and regulations. All data, e-mails, e-mail attachments, documents and other electronic information within the County network/e-mail system are the property of Gillespie County.

**THERE IS NO EXPECTATION OF USER PRIVACY OR CONFIDENTIALITY IN COMPUTER NETWORK USE, INTERNET ACCESS AND E-MAIL USE ON THE COUNTY'S SYSTEMS.**

The County, acting through its Elected Officials and Department Heads, has the capability to view User data and e-mail at any time. Whereas all County employees are allowed access to the Internet, only full-time employees are provided e-mail accounts within the County's system. Part-time and temporary employees are not granted a County e-mail address by default. If a need exists for said part-time and temporary employees to have access to the County e-mail system, the Elected official or Department head should express that to the IT Director who will determine if there are sufficient unallocated e-mail licenses. The IT Director shall have the final decision in the allocation of County e-mail resources. This policy does not supersede any state or federal laws regarding confidentiality and appropriate use of County resources.

The primary purpose of using the County's Computer or Telephone network, Internet and e-mail system is to advance the business of the County. This includes, but is not limited to:

- Communication with, and providing services to the citizens, visitors, and clients of Gillespie County.
- Conducting the business of your department or unit
- Communicating with other employees for work-related purposes.
- Gathering information relevant to your duties or to expand your expertise.

Access to and use of the County's computer network, Internet and/or e-mail systems of the County shall always be lawful, ethical, reflect honesty, and show restraint in the consumption of shared resources. Users shall refrain from monopolizing systems, overloading networks with excessive data or wasting computer time, connect time, disk space, printer consumables, manuals, or other resources. County Users may be subject to

reasonable limitations on their use of the networks, or other action, as determined by the IT Director. Users are also expected to cooperate with any reasonable investigation regarding User access to and use of the County's computer network, Internet and/or e-mail systems of the County.

Content of all electronic communications should be accurate. Users should use the same care in drafting email and other electronic documents as they would for any other written communication.

As with internal e-mail messages, Internet e-mail can be changed by outside parties and forwarded to others without the employee's knowledge or permission. Users must use caution in using Internet e-mail and must comply with all state and federal laws. Unauthorized access or interception of another person's e-mail is a violation of state and federal law and will be reported to the appropriate authority for investigation and possible prosecution.

User data and documents are a County asset and should be treated as such. For this reason, Users who have access to OneDrive/SharePoint or a NAS device should store all data files in these locations as these files are backed up continuously. Recovery of data stored locally on desktops is the User's responsibility. Storage only on a desktop or laptop hard drive is a risk in that if the hard drive fails, the data may not be recovered.

## 6.1 Limited Personal Use

Authorized Users of the County may also use the Internet and e-mail for **limited personal use**. This is defined as any personally initiated online activity (including e-mail and Internet usage) that is conducted for purposes other than those listed above. ***This is a privilege***, not a right, and may be limited or removed at any time. Gillespie County disclaims any liability for any loss or damage suffered by an employee because of that employee using the County Internet connection for personal use. Occasional, limited, appropriate personal use of the County computer system is permitted when the use does not:

1. Interfere with the User's work performance.
2. Interfere with the normal operation of your department or work unit.
3. Interfere with any other User's work performance or have a negative impact on overall employee productivity.
4. Have a negative impact on the operation of the computer system.
5. Cause any additional expense or load to the County or department.
6. Compromise any department or the County in any way.
7. Violate any other provision of this Policy, any other policy guideline, or any local, State, or Federal law or regulation (e.g. HIPAA; CJIS).

## 6.2 Inappropriate Use

The use of a public resource for private or personal gain, and/or any excessive private use of public resources, by any User is absolutely prohibited and punishable by applicable County disciplinary procedures, which may include termination and/or criminal prosecution. The term "public resource", as used in this Policy, includes use of County equipment, hardware, software, or tangible articles, and any employee time ("on the clock") expended in the use of a public resource.

Examples of unauthorized use of public resources include streaming music or video, stock tickers, news reels, movie downloads, games, screensavers used from the Internet, unauthorized messaging software such as AOL, YAHOO, Windows Messenger; and "chat" software, except when any above listed use is necessary for conducting County business.

Users shall not:

1. Use IT resources for personal gain, or to support or advocate for non-County related business or political purposes.
2. Create, distribute, upload, or download any disruptive, abusive, harassing, threatening, or offensive messages, including offensive comments or graphics about sex, race, gender, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
3. Use IT resources for illegal or unlawful purposes or to support or assist such purposes.
4. Use IT resources for wagering, betting, or selling chances or to support or assist such purposes.
5. Use IT resources for personal long-distance telephone calls.
6. Attempt to circumvent or subvert system or network security measures, provide internal network access to any non-Users, or use your account to gain unauthorized access to external networks and systems.
7. Mount an attack on the security of any system (i.e., attempting to hack or introduce viruses into a system).
8. Use the County network to disrupt network Users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer "worms" and viruses, and sustained high volume network traffic that substantially hinders others in their use of the network.
9. Intercept network traffic for any purpose unless engaged in authorized network administrative duties.
10. Install or use encryption software on any Gillespie County computers without first obtaining written permission from your Department Head and the IT Director. Users may not use encryption keys or encryption passwords that are unknown to their Department Head.
11. Engage in online fundraising (unless approved by Department Head or Elected Official)
12. Engage in mass-mailing or send County-wide messages without Department Head or Elected Official approval.
13. Send County-wide mailings about viruses, or other warnings about outside computer attacks (these are almost always a hoax and should be turned over to IT for disposition).
14. Initiate or forward chain letters by email.
15. Spoof (disguise) your identity or send anonymous e-mails or send e-mail under another person's name without permission.
16. **Download any non-standard or non-business-related files or software, including "freeware" and/or "shareware" programs, unless previously approved by the IT Director.**
17. Load personal Internet Service Provider accounts on County owned equipment.
18. Send, transmit, or otherwise disseminate proprietary data, trade secrets, or other confidential information of the County without authorization. Unauthorized dissemination of this information may result in substantial civil liability and/or criminal.
19. Make or use illegal copies of copyrighted software or other mediums, store such copies on County systems, or transmit them over the County network.
20. "Rip" music CDs and store said music on County owned equipment, computers, or servers.
21. Store any personal documents that have no relevance to any County business on any County owned equipment, computers, or servers.

It is the shared responsibility of all County employees, supervisors, managers and/or department heads, and IT, to be aware of how the County's Internet resources are being utilized by his/her employees.

## 6.3 Network Monitoring

All computer applications, programs, data, and work-related information created or stored by County employees on County information systems and resources are the property of Gillespie County. Gillespie County employees shall have no expectation of privacy in anything they store, send, or receive on the County's computer systems. Data may be monitored without prior notice. IT reserves

the right to access and monitor e-mail use and any other computer-related transmissions, as well as stored information, created or received by County Users with County IT systems and resources under the following circumstances:

1. Performance monitoring or problem-solving purposes
2. Necessary during an investigation for possible violation of County policies
3. There is reasonable suspicion that a User has committed, or is committing a crime, an act against the best interests of the County, or an act for which the County could be liable
4. Random or automated monitoring to ensure that content is in compliance with the County's established policies.
5. Request for monitoring is made by appropriate authority
6. Required to do so by law

The reservation of this right is to ensure that public resources are not being wasted and to ensure the County's information systems are operating as efficiently as possible to protect the public's interests. This includes blocking access to certain Web sites for which access is deemed to conflict with County policy.

## 6.4 E-Mail Records Retention

Depending on the content of an e-mail message, it may be considered a formal record and need to be retained pursuant to a department's record retention schedule.

Users are cautioned that deleting an e-mail message from a User's own mailbox does not mean all copies of the message are also deleted. The message may still reside in the recipient's mailbox, may have been saved in some other folder, or forwarded to other recipients. Also, any message sent may be saved in a system backup and retained.

IT will NOT be held liable for any e-mail that is deleted that should have been retained pursuant to a records retention schedule. It is the sole responsibility of the User to ensure that they comply with any applicable records retention schedule.

As with other records, no County e-mail record may be destroyed after it is requested for reasons related to employee termination, disciplinary action, or contemplated or pending litigation, until destruction is approved in writing by the County Attorney or outside legal counsel representing the County in the matter.

Managers and supervisors may, with Department Head approval, access, as necessary, another employee's e-mail if employees are on leave of absence, extended leave, or are transferred from one department to another.

## 6.5 Data Storage

IT provides access to SharePoint (department) and OneDrive (individual) for employees to store their data. These are cloud services in Microsoft's Government Cloud. These services backup data continuously to ensure its integrity and availability. However, these storage resources are limited. IT asks that Departments and Users practice good housekeeping by only storing files in these locations as long as is necessary to comply with applicable statutes, regulations, or business needs.

IT is NOT responsible for loss of any data that is not stored in the designated data storage areas.

## 6.6 Cloud Storage

Any data owned by Gillespie County that will be stored in any Cloud environment MUST be stored in a Government Cloud Service Provider (GCSP) such as Microsoft or AWS Government Clouds. Departments or Users must NOT use any other cloud storage service ( e.g Google Drive, IDrive, Dropbox). Department Heads who have a need to deviate from the standards must request an exception. The IT Director will review the request and either approve the request as is or suggest alternate solutions to ensure compliance with state and federal law and County IT security.

# 7 Security

Gillespie County has a comprehensive computing environment that encompasses a broad array of networking, server, and desktop computing platforms as well as the complimentary systems software. Users should never consider electronic communications to be either private or secure. E-mail and data could potentially be stored indefinitely on any number of computers, in addition to that of the recipient. Copies of email messages or altered messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to nonexistent or incorrect Usernames may be delivered to persons that the sender never intended.

Each User is responsible for ensuring that his or her use of outside computer and networks, such as the Internet, does not compromise the security of Gillespie County's computer network. This duty includes taking reasonable precautions to prevent others from accessing the County's network without authorization and to prevent the introduction and spread of viruses.

## 7.1 Network / Internet Security

Standards and requirements exist to ensure security and availability of the data and systems. The County's network connects to the Internet through a firewall and Intrusion Prevention System (IPS).

The County also employs a web content filtering system in an effort to ensure that County internet resources are not being misused. Examples of misuse would be visiting websites for extended periods of time, or repeatedly that have no value or relevance to the operation of business activities of Gillespie County. Department heads can request that sites become black-listed by the IT Director, and the IT Director shall make every effort to investigate the feasibility of such a block.

At times there may be other technology that will be employed by departments for the operation of that department. It is the IT Department's responsibility to always ensure network security. It is required that before ANY technology is connected to the County's network, that was not procured by IT, the IT Director should be contacted and be present at any meetings with the vendor prior to purchasing and installation of said technology, in the interest of network security. Failure to follow this guideline can result in denial of installation of said equipment / software.

**Non-County owned laptops or mobile devices cannot be used to connect to any County system that contains CJIS or HIPPA data.** Personal devices are not to be connected to the County's wired network. All non-county-owned devices must use the County Wi-Fi Network.

**Security Patches -**The County has a process to update all servers and PCs with the latest security patches to enhance security. Any application vendors should adhere to the industry practice of compliance to the latest version of system software levels to ensure maximum security to information and services provided by the County.

**Network Devices** – Prior approval from IT must be obtained before any of the following activities are attempted:

- Connecting any networking devices to the County network.
- Usage of modems on individual servers / desktops /workstations for remote access purposes.
- Allowing non-county agencies or entities to access the County network without prior IT approval.

- ***Allowing ANY person who is not employed by Gillespie County access to any computer or private network connection.***

The following activities should only be carried out by IT, or its authorized designees:

- Connecting networking devices to the County network.
- Interconnecting external networks by routers or VPN.

To maintain the security of the County network, all the Virtual Private Network (VPN) Users should ensure that:

- Their County PC has the most current virus protection installed
- Operating system has all the recommended patches installed
- Browsers have all the recommended patches installed.

**Security Issues –** The Gillespie County Information Technology Services department has several levels of potential security related issues, such as security breaches, or violations, that should all be handled in the appropriate manner according to severity.

- **Level I Incident -** User feels that their Username and/or password have been compromised and feel that an unauthorized person can gain access to the County's computer system with their account. Employee is suspected sharing of User account information with other Users and or non-employees.
- **Level II Incident -** Involuntary employee termination or Employee arrest**.**
- **Level III Incident -** Suspected Computer break-in or computer virus**,** Loss or suspected compromise of VPN password**,** Physical Intrusion (unauthorized entry of both criminal and non-criminal type)**,** Disaster or any form of major damage at computer site (Gillespie County Courthouse Jail Data Processing Room and Gillespie County Sheriff Office), or Sudden employee resignation.

**Actions to take upon level of severity** – The following should be followed upon learning of a security issue guided by the severity set forth above.

- **Level I Incident –** Notify the Gillespie County Information Technology Services Department within one working day of the suspected violation. IT will then determine the action required, if any, from the User.
- **Level II Incident** – Notify IT and County Attorney's Office within one hour of the security issue, at which time the IT staff will take appropriate actions to suspend or terminate the User's account.
- **Level III Incident** – Notify IT immediately of the incident, regardless of time of day, by the appropriate means of contact. The IT staff will then immediately rectify the situation or respond to the location the issue occurred.

The IT Director may remove computer access from any User account that could potentially constitute a security breach of the Gillespie County System for any of the above reasons, WITHOUT notice or request from an Official or Department head, if the potential security breach could compromise the data and network security of the County network (e.g., computer virus, backdoor, data collector, employee arrest, sudden resignation)

**If contact cannot be made with the IT director, contact the Gillespie County Communications Center, who will always have contact with the IT director or IT Technician for Level III incidents.**

## 7.2 Anti-Virus Protection

The County network is protected from viruses with the help of firewalls, e-mail scanning software and desktop scanning software. However, Users must follow these guidelines:

In some cases, simply reading an e-mail can spread a virus to a User's computer, and from there to many other internal and external County recipients. The County will take prudent measures to scan incoming e-mail and attempt to intercept viruses. However, no safeguard is foolproof, and viruses can find their way into County Users' computers from a variety of other ways (e.g., USB drives, internet file transfers). Each User is responsible for taking reasonable precautions to avoid introducing viruses into the County network, including but not limited to:

- Always run the County standard, supported anti-virus software that the County provides.
- NEVER open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Recycle Bin.
- If you receive an email with an attachment from someone you know, verify the email and attachment is something you were expecting. If not, then contact the sender to verify that the attachment was something they intended to send.
- Delete and never forward spam, chain, and other junk e-mail.
- Never download files from unknown or suspicious sources.
- Avoid USB drive sharing with read/write access unless there is absolutely a business requirement to do so.

**Viruses and Laptops/Mobile Device**

Viruses can gain back door entry via laptops and mobile devices that are normally outside the network, and which may get infected. To eliminate such risks, the following guidelines should be used while using laptops on the County network.

1. Always make sure that you have current antivirus protection on the laptops. County provided laptops should have CrowdStrike antivirus software on them. If it is not present, please contact IT.
2. If connected on the county network, antivirus updates for this software are continuous. All other county laptop Users should ensure that they periodically, (monthly) connect the laptops to the county's network overnight to get the antivirus updates.
3. Scan your hard disk periodically for any virus. Once a week is an ideal frequency as this would help the ongoing detection of any virus, or new virus, on your machine.
4. If required, IT will schedule a maintenance window with the department head to turn in their laptop to be scanned and updated.

Following these steps while using your laptop or mobile device will help ensure the safety and security of the County's data and network. For questions, please call the IT Department.

## 7.3 WIFI

Wireless access is available at all County facilities. The "gcdevice1" network is for use by County Employees only. "GC Guest" networks can be used contractors or the public while doing business at County facilities. Connectivity to the guest networks is limited to one day.

## 7.4 Remote Access

IT has limited resources for remote access. For remote access into the Gillespie County network, the User MUST use a Gillespie County owned laptop that is pre-setup for the employee to use. The User or User's department head must show a need for the purpose of remote access.

IT utilizes Beyond Trust (Bomgar) for remote access to County resources. All Users and vendors MUST use this service when remotely accessing Criminal Justice systems.

## 7.5 IDs & Passwords

Passwords are an important aspect of computer security. They are the front line of protection for User accounts. A poorly chosen password may result in the compromise of Gillespie County's entire network. The scope of this policy includes all personnel, including third parties, who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Gillespie County facility, has access to the Gillespie County network, or stores any non-public Gillespie County information. As such, all are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Users are responsible for safeguarding their passwords for access to the computer system. Users are responsible for all transactions made using their passwords. No User may access the computer system using another User's password or account without expressed permission. No User may portray oneself as another User.

In order to provide appropriate network security, this policy mandates that County IT utilize passwords and periodically require Users to select a new password. Although Users have confidential passwords, this should not be construed to mean that the application data is the property right of the User or that network, internet nor that e-mail access is for personal confidential communications or that the password is to protect the employee's privacy.

Users are expected to follow these guidelines:

- Passwords shall remain confidential and should not be printed, stored online or given to others.
- Passwords for Criminal Justice resources are required to be changed every 90 days, all other systems may require periodic changes.
- Passwords shall be at least eight characters long.
- Passwords shall contain characters from at least three of the following four classes: (i) English upper-case letters, A, B, (ii) English lower-case letters, a, b, (iii) Westernized Arabic numerals, 0,1,2, and (iv) non-alphanumeric ("special characters") such as punctuation symbols.
- Passwords may not contain your Username or any part of your full name.
- Passwords must not be transmitted in the clear outside the secure location.
- The password shall not be a word found in a dictionary (English or foreign) or a proper name.
- The password shall not be identical to the previous ten (10) passwords.

## 7.6 Third-party Access

This policy establishes the rules and responsibilities for third-party access which:

1. Gillespie County employees who are responsible for the contracting and/or supervising of the third party and
2. third-party access to Gillespie County information systems and the data center.

A third-party is any individual from an outside source (contracted or otherwise) who is granted access to County information systems. A third party could consist of, but is not limited to, software vendors, contractors, consultants, business partners, and security companies.

- A third-party does not have unattended access unless defined by contract along with rules of access.
- Remote Access software the third-party uses shall be approved by the IT Director of Gillespie County (CJIS systems MUST use Bomgar).

ALL Third-party access, or outside consultants MUST be approved by the IT Director of Gillespie County, before access is granted.

## 7.7 Desktop Security

Please follow the guidelines below to avoid security breaches:

- Close sensitive or confidential applications and lock your workstation when you leave your desk.
- Do not leave portable media unattended such as CDs or USB drives.
- Log off your computer when you leave for extended periods.
- Never write your passwords on a sticky note nor try to hide them anywhere in your office.
- Remove printouts from printers before leaving your office.
- Shred sensitive printouts or paper when you are done with them (subject to any records retention requirements).
- Use a screen filter to minimize the viewing angle on a computer monitor, where appropriate. Enable a password-protected screen saver. Clear cache files on computer and memory on devices like printers regularly.

## 7.8 Portable Memory

The use of USB flash drives, small, keychain-sized storage devices or other portable memory is discouraged due to the portability of viruses. NEVER use a USB storage device of unknown origin in any County computer system. If there is any doubt about a device's security status, inform IT immediately so the device can be inspected and securely erased.

## 7.9 Computer Data Backup

For all servers in the County's Jail data center, the following backup policy is administered.

**Server Backup:** Every day each vital server is backed up to a backup appliance located in the IT data center. This includes the application files and data files. Individual workstations are not backed up to this appliance. Backups occur at night so any new data lost between backups cannot be recovered.

**Retention Policy:** Server backups are retained for a 30 days duration (7 daily, 5 weekly, 1 monthly).

**User Data Backup:** IT provides access to SharePoint (departmental backup) and OneDrive (individual PC backup) for employees to store their data. These are cloud services in Microsoft's Government Cloud. These services backup data continuously to ensure its integrity and availability. They allow Users to quickly recover from a crashed computer by not having their data located directly on their computer. Users are STRONGLY encouraged to participate in this method of data storage.

IT is NOT responsible for loss of any data that is not stored in the designated data storage areas.

## 7.10 Security Access Removal

**Computer System Security:** Department heads shall notify IT immediately of when a User is or will be terminated so their computer and email account can be deactivated. A terminated employee's email will be archived for 30 days before deletion, unless the department head requests an extension.

Persons no longer employed have no right to the contents of their e-mail messages or data stored in County systems and shall not be allowed access to the internal County system.

### 7.11 Retirement/Destruction

All computers, network equipment, and peripherals replaced will be reviewed to see if it can be recycled for County use or if it must be retired. The recycling of a device is determined by whether it will support the current operating system and run without error.

All computers that are brought into IT will have the hard drive removed and held for a minimum of 90 days. This includes SSD drives, mechanical drives, and M.2 Storage devices. After 90 days, if the drive can be reused, then it will be formatted and held as a spare. If the drive is obsolete, it will be destroyed. All other equipment deemed obsolete will be disposed of per applicable Texas law.

### 7.12 Related Laws and Statutes

The State of Texas has established laws relating to computer and electronic security and crimes related thereto. Texas Penal Code Chapter 33 details the definitions, offenses, and penalties for computer crimes committed in the State of Texas. All logged computer transactions are logged by a User's access credentials (i.e. Username / password). Users of the County network shall NOT give ANYONE their password or Username, for both security of the county network and to protect the User. Different Users inside departments may have different levels of access to the computer system, and by sharing their password, a security risk is introduced, and possible violation of criminal / civil law may occur.

Texas Penal Code Chapter 16 relates to the interception of electronic communications including telephone "tapping", interaction of electronic mail (e-mail), interception of telephone calls, and disclosure of said information.

## 8 Weather Emergencies and Protection of Computer Equipment

Upon activation of the Emergency Operations Center (EOC) for weather emergencies the following steps are to be taken by each User to help protect both computer hardware and software.

- All computer equipment should be powered off. This applies to personal computers; workstations, printers and any associated peripheral devices (i.e., scanners, etc.). After powering down the equipment, disconnect the power cables from the receptacles to protect equipment from potential surges from lightning.
- Any equipment located on the floor should be moved to a higher location and away from any windows. All monitors should be turned so that no screens face the direction of any windows.

## 9 Policy Infraction

County employees who violate this policy may have their computer system access revoked and may also be subject to disciplinary action, up to and possibly including termination. Other legal remedies, including civil and criminal prosecution, may also be pursued if warranted.

It is the policy of Gillespie County to handle policy infractions as follows:

1. The violation shall be reported to the User's supervisor or manager.
2. The User's supervisor should approach the violator(s) directly with the findings, ensure the User is aware of the policy, and give them the opportunity to cease and desist; or, depending on the severity, follow disciplinary procedures consistent with the guidelines and policies of "*Gillespie County Employee Handbook*."

# 10 Computer Support / Technology Requests

## 10.1 Help Desk

Information Technology Services offers support for existing County computer systems by calling 888-992-9986. Non-emergency support can be obtained by emailing techhelp@gillespiecounty.org and will be performed during business hours, 8:00am-5:00pm, Monday through Friday. Emergency support is provided 24/7 (Sheriff's Office and Communication Center) through the 888 number above.

# 11 Definitions

- Attachments - Files created in other applications (such as Word, Excel).
- CJIS - Criminal Justice Information Services. CJIS is the FBI division responsible for the collection, warehousing, and dissemination of relevant criminal justice information to the FBI and law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.
- E-Mail - An electronically transmitted message, along with any attachments and any information appended by the e-mail system.
- E-Mail System - Computer hardware and software system that allows personal computer Users to send, receive and store messages, documents and files with other individuals or groups of people over an internal network or the Internet.
- Employee – Any person who is currently on the Gillespie County payroll and works in a County office. Any elected or appointed County official.
- Encryption - A means of coding messages so they appear to be random characters. Encryption has two benefits. First, it prevents disclosure of sensitive information to unauthorized third parties. Second, encryption allows for "authentication" of the information sent.
- Freeware - programming that is offered at no cost, which is copyrighted so that one can't incorporate its programming into anything one may be developing.
- Hacking – the unauthorized attempt or entry into any other computer or system.
- HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.
- Internet – a worldwide computer network through which you can send a letter, chat to people electronically or search for information on almost any subject you care to think of. Quite simply it is a "network of computer networks".
- Internet Browser - an application that displays HTML and other information found on the Internet. Google Chrome, Edge, and Firefox are examples of browsers. This type of client software accesses the World Wide Web and lets you drift from link to link without having to have a purposeful search.
- Internet Service Provider (ISP) - an entity that charges startup and monthly fees to Users and provides them with the initial host connection to the rest of the Internet usually via a cable or fiber connection.
- Intrusion Alarm System – An electronic system that is designed to detect unauthorized entry into a building or secure location during a set time period and to report any unauthorized entry to the appropriate authority.
- IT - Information Technology Services Departmental label referring to the employees of Gillespie County Information Technology and current information technology outsource vendor.
- Panic System - A system installed that is used to immediately report danger or request officer assistance due to an unforeseen or unknown situation. The panic system is created utilizing PC app "panic buttons" that, when activated, cause a message to be displayed on the Communication Center's monitors.
- Public Record – as defined in Texas Open Records Act.
- Public Resource - Includes not only County equipment, hardware, software or tangible articles, but also the employee's time expended while on duty with the County.

- Risk - Those factors that could affect confidentiality, availability, and integrity of Gillespie County's key information assets and systems. Gillespie County is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.
- Shareware - software that is distributed free on a "trial basis" with the understanding that the User may need to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date (after 30 days, the User can no longer get access to the program). Other shareware (sometimes called liteware) is offered with certain capabilities disabled as an enticement to buy the complete version of the program.
- Third Party – Any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.
- Trade Secret **–** as defined by law.
- World Wide Web (WWW) - a hypertext-based distributed information system for linking databases, servers, and pages of information available across the Internet.

RELEVANT PENAL CODE AND OTHER STATUTES

1.) Texas Penal Code CHAPTER 33. COMPUTER CRIMES

2.) Texas Penal Code CHAPTER 16. CRIMINAL INSTRUMENTS, INTERCEPTION OF WIRE OR

ORAL COMMUNICATION, AND INSTALLATION OF TRACKING DEVICE

3.) USC – Electronic Communications Privacy Act

4.) CJIS Security Policy Manual sec. 4.2.5.2 dated: July 2024 (Version 5.9.5)

5.) The Health Insurance Portability and Accountability Act of 1996 (HIPAA) CFR part 160 and 164

6.) Other related State and Federal Law

---

**12 User Signature of Acknowledgment**

Use of any equipment that will be connected to, accessing, storing data on, transmitting any data across, or any other use of the computer network owned and operated by Gillespie County, constitutes acceptance of the practices, restrictions and guidelines set forth in this Policy.

I, _____ have read, understand, and acknowledge that I will abide by this Technology Usage Policy while employed, affiliated with, or doing business with Gillespie County.

Signature: _____ Date: _____

Received by:
Department Head/Elected Official

Signature: _____ Date: _____

Human Resources

Signature: _____ Date: _____