Rusk County Information Technology Policy

by

Willis Marlin - IT Director

1 Purpose

The purpose of this policy is to provide guidance and set forth the acceptable use of County Technology Resources by users at the County of Rusk ("County") to ensure resources are used in an appropriate, responsible, and lawful manner that protects the County and serves its interests.

2 Scope and Applicability

This policy applies to all County employees, officers, elected officials, appointed officials, contractors, consultants, temporary workers, interns, volunteers, and vendors ("Users") who are provided access to County Technology Resources.

The policy covers the following topics pertaining to use of County Technology Resources:

- Definitions
- General
- E-Mail
- Internet
- Network and Cybersecurity
- Computer Equipment and Software
- Mobile Devices
- Any type of device that uses, accesses or creates data or technology related information
- Data and Information
- Telephones and Voicemail
- Technology Purchases
- Separation or Discontinuance of Services

- Netiquette
- Violations

3 Definitions

The following definitions apply to this policy.

a. County Technology Resources

County Technology Resources refers to the County's computing and communications environment and resources used to create, process, store, and transmit data and information, including, but not limited to, the County's network (wired and wireless, including guest Wi-Fi), electronic mail system (e-mail), internet service, desktop and laptop computers, systems and applications software, data, storage, mobile electronic devices, including smartphones and tablets, cell phones, telephone system and telephone handsets, voice-mail system, pagers, printers, copiers, facsimile machines, scanners, audio *I* video equipment, social media, and cloud-based and third-party software and infrastructure services. This may also be referred to as the County's computing environment or Information Technology systems.

b. Texas Public Information Act

The Texas Public Information Act (TPIA) is a Law under Texas Government Code Chapter 552, gives you the right to access government records; and an officer for public information and the officer's agent may not ask why you want them. All government information is presumed to be available to the public. However, certain exceptions may apply to the disclosure of the information. Government bodies shall promptly release requested information that is not confidential by law, either constitutional, statutory, or by judicial decision, or information for which an exception to disclose has not been sought.

Please go to sos.state.tx.us/records.shtml for information regarding what may be withheld due to exception.

c. Confidential Information

Confidential Data and/or Information is privileged information for a designated purpose that is only intended for recipients with a business need-to-know. Some examples include certain personal information such as medical (e.g.: HIPPA), personally identifiable information (PII), recruitment, disciplinary, and performance information; attorney-client privileged communications; and protected information. Unless exempted by law, some types of confidential information may be subject to

legal inspection and/or disclosure requirements.

d. Contractor *I* Vendor

An independent person or business contracted to perform services for the County.

e. Copyright

The exclusive legal rights to copy, reproduce, or sell a specific piece of intellectual property.

f. Encryption

The coding or scrambling, using sophisticated techniques, of information to prevent third parties from "reading" or accessing it.

g. Exempt Employees

Employees who are not subject to the minimum wage and overtime provisions of the Fair Labor Standards Act.

h. Intellectual Property

Refers to a number of types of creations such as books, movies, songs and software. Intellectual property is protected by a body of law collectively referred to as copyright law.

i. Malware

Any Malicious software intending to cause harm and disruption to County Technology Resources. Examples include, but are not limited to, viruses, worms, Trojan horses, spyware, dishonest adware, and ransomware.

j. Mobile Device

An electronically-powered portable device that can view, process, store, and transmit data wirelessly using cellular, radio, satellite, or another communications technology. Examples
include smart phones, tablets, laptops, Personal Digital Assistants (PDAs}, and cell phones. Also referred to as Mobile Electronic Device.

k. Personal Mobile Device

A Mobile Device that is personally owned by a User that is authorized to use County Technology Resources. This may also be referred to as Bring Your Own Device (BYOD).

l. Mobile Device Management (MDM)

A system used to administer the management, support, optimization, functionality, and security of mobile wireless devices necessary for the deployment, security, monitoring, and integration within the County's computing environment.

m. Network

The collective name for equipment, devices and digital resources that interchange information using a common medium.

n. Non-exempt Employees

Employees who are subject to the minimum wage and overtime provisions of the Fair Labor Standards Act.

o. User

County employees, elected officials, contractors, consultants, temporary workers, interns, volunteers, vendors or anyone that is provided access to the County's Technology Resources.

4 General

a. Background

The County utilizes County Technology Resources in every department to support the delivery of public services to County residents, businesses, and the community. Technology is a core element to the effective operation of the County. As such, it is important to have standards in place for its proper use to maximize its reliability, integrity, and performance. As with other finite public resources, County staff should be responsible stewards of these resources. These resources should be used judiciously, responsibly, and appropriately.

The County is the custodian of data and records processed and stored in its information systems. In addition to public information, there is sensitive and confidential data. The County is responsible to protect and safeguard its data and systems from unauthorized access, corruption, and loss.

Technology solutions and deployment models continue to evolve and become increasingly complex. The County's technology environment includes a hybrid of on premise and cloud-based solutions. Many County systems utilize the Internet in some way, and many are integrated and inter-dependent upon one another. Computer operating systems, applications software, and hardware firmware are continually being updated to provide improvements and bug fixes. Increased internet connectivity, inherent vulnerabilities in systems, and new malware and cyberattacks expose County information systems and data to increasing threats.

This Technology Use Policy puts in place rules and expectations for responsible use of County Technology Resources to optimize value, reliability, integrity, and performance of County information systems, comply with laws, reduce risk of loss and exposure, and protect the County, its image, and interests. Users are required to comply with the provisions of this policy. The County will provide training relative to this policy in various methods and as needed. Any variations from this policy, must be authorized in writing by the IT Director and County Commissioners Court.

b. <u>No Expectation of Privacy</u>

County Technology Resources are the property of or placed into service for use by the County. Users have no reasonable expectation of privacy in the use of County Technology Resources. The Texas Electronic Communications Privacy Act does not apply.

At any time and without prior notice, the County may monitor and examine e-mail, website access, network and internet activity, computer files, and other information transmitted through or stored on County Technology Resources.

Logs are recorded for accessing various County Technology Resources such as, but not limited to, network and systems, websites, email, and data *I* electronic transactions.

Records, regardless of form, pertaining to the conduct of County business are subject to the Texas Public Information Act (TPIA) and may be publicly disclosed.

Records may also be discoverable and disclosed as allowed under law in the event of litigation.

County Technology Resources, such as assigned computers or mobile devices, may be subject to seizure or subpoena in criminal or civil investigations or cases.

c. <u>Acceptable Use</u>

County Technology Resources should be used for conducting County business. Examples of allowable use of County Technology Resources include the following:

- To facilitate the performance of job *I* service functions.
- To facilitate the communication of business-related information.

- To coordinate meetings of individuals, locations, and County resources.
- To store and access County documents and data related to County projects and functions.
- For research and education required to perform job / service functions.
- To communicate with departments, outside individuals and organizations in order to perform a job / service function.

Incidental personal use of County Technology Resources is acceptable as long as it does not interfere with the normal performance of a User's work duties or over-burden County resources. Personal use should be kept to a minimum.

d. <u>Prohibited Use</u>

Prohibited use of County Technology Resources include, but are not limited to the following:

- Illegal activities.
- Making threats, harassment, slander, defamation, promotion of violence or hate.
- Obscene or sexually explicit images or communication.
- Use of hardware, software or data of any sort or type with malicious intent.
- Intentionally causing disruption, damage, or loss to County Technology Resources.
- Violation of copyright laws.
- Using unlicensed software.
- Installing non-work-related software.
- Installation of non-County hardware or software not authorized in advance by the IT Director.
- Copying County-owned software for personal use.
- Unauthorized access to networks, systems, services, files, data, e-mail or voice-mail.
- Providing or enabling of others to have unauthorized access to networks, systems, services, files, data, e-mail or voice-mail.
- Political endorsements, solicitations, or private use.
- Union business use must be consistent with the limitations for incidental personal use, as indicated under section 4.3 and only during nonworking

time. The County will comply with applicable legal requirements consistent with State and Federal Law concerning use of County technology for union business.

- Gambling and game playing.
- Personal gain, private use, working for another business, or commercial activities.
- Storage of personal music, videos, photos or files.

e. Downloading or Opening Internet Files or E-mail Attachments

Downloading or opening files from the Internet or e-Mail attachments expose the County to potential harm from malware. Although County Windows-based computers have anti-virus software installed, this software does not protect from all malware.

1 Users should not download or open flies on the Internet unless there is a business purpose.

2.Users should exercise extreme caution when downloading or opening files from the Internet or in e-mail attachments. When in doubt users should contact IT department staff.

3.Users should NOT download or open executable files or attachments. Common executable files have the following extensions (the last 3 letters after the last dot). This is not an exhaustive list.

- Programs: .exe, .com, .msi, .msp, .cpl, .hta, .jar, .pif, .scr, .application
- Scripts: .bat, .cmd,.vb, .vbe, .vbs, .js, .jse, .ps1, .ps2, .ps1xml, .ps2xml, .ws, .wsf
- Shortcuts: .scf, .lnk, .inf; Registry: .reg
- Microsoft Office files that contain macros: .docm, .dotm, .xlsm, .xltm, .pptm

4. Users should not download or extract compressed or archived files from the Internet or in e-mail attachments without prior IT Department authorization and possible assistance. Compressed files may have malicious executables within them.

   Common compressed file extensions are .zip, .7z, .rar,,.rOO, .r01, etc.

5. Users should contact the IT Department if uncertain about downloading or opening a file or e-mail attachment.

f. Representation

Use of a County e-mail address or IP address represents the County when communicating with an external party or using an external service, such as a newsgroup, bulletin board, or listserv. Users authorized to interact with external parties or services should conduct themselves professionally and appropriately within the context of their role and *I* or authority at the County. Refer to the County's Social Media Policy referenced below for additional policies governing use of County social media sites and communications on such platforms on behalf of the County.

g. Good Judgement

Users should use common sense and reasonable judgement when using County Technology Resources. This section 4.7 does not abrogate the provisions of any other section of this policy.

h. Revisions and Related Documents

This policy may be updated and revised from time to time. Updates will be available upon request and posted on the County's internal board.

5 E-Mail

a. Authorization

1. Users must receive authorization from their supervisor or sponsoring Department Head (Director) to obtain a county e-mail account.

1.

2.Remote access to the County's e-mail system from the Internet using a web browser {e.g.: Outlook Web Access) and *I* or a mobile device (e.g.: smartphone, ActiveSync) requires authorization from the User's Department Head or designee and the IT Director.

3.Non-exempt hourly employees are prohibited from checking or accessing County e-mail during off-duty hours unless pre-approved by the employee's supervisor. Non-exempt employees will be compensated for any approved overtime.

b. General E-mail Provisions

1. Users are to only use County e-mail accounts when sending messages pertaining to County business.

2. Use of personal e-mail accounts for County business should only be used on an exception basis {e.g. offsite with no access to County e-mail, emergency situations). Or in such a case where part time or an intern is in-house In such a case, the User's County e-mail address or an appropriate County e-mail address should be copied (cc'd).

3.E-mail messages sent from County e-mail addresses *have* the same effect as communicating on County letterhead.

4.E-mail messages sent from County e-mail addresses or pertaining to the conduct of County business should be professional and business-appropriate.

c. Disclosure

1. E-mail messages pertaining to the conduct of County business are subject to the Texas Public Information Act (TPIA) and may be publicly disclosed unless exempt by law. This applies to e-mails using County Technology Resources as well as personal e-mail accounts and/or from personal devices.

2.Users are required to provide to the County copies of any e-mail messages in their personal e-mail account(s) and *I* or devices that pertain to the conduct of County business that are responsive to a TPIA request except as exempt by law.

3.E-mail messages may also be discoverable and disclosed as allowed under law in the event of litigation or a criminal investigation.

4.The County may archive e-mail messages of County e-mail accounts. Archived e-mail messages will be retained per the County's e-mail retention policy *even* if a User deletes messages from their email software client (e.g.: Microsoft Outlook). Archived e-mail messages are subject to the TPIA except as exempt by law.

d. Special E-mail Access Authorization

1.It may be necessary for a User to access another User's e-mail account under special circumstances. In such a case, the Department Head must authorize access by submitting an E-Mail request to the County's IT Director.

2.Special entry involves overriding the standard County e-mail system

security controls by a member of IT to change an account password to a new password and to provide that password to authorized individual.

e. Global E-mails

1.Global announcements that are to be sent to all County email users ("global e-mails") must be approved in advance by the County Judge or IT Director or a designee.

f. Mailbox Storage Size

1. Users are responsible for managing and controlling the contents and size of their County e- mail mailbox.
2. User e-mail mailbox storage will be limited to a maximum size threshold identified by TAC licenses.
3. Warning messages will be sent if the e-mail account maximum storage size is being approached.
4. If the maximum storage size of an e-mail mailbox is reached, the e-mail User will be notified and e-mail service will be suspended. The service suspension will continue until the e-mail account storage size has been reduced below the maximum size threshold.
5. Users who have a justifiable business requirement for mailbox storage size in excess of the County standard size may submit a request to their perspective Department Head for authorization which will be submitted to IT Director.

g. E-mail Retention

1. Purpose of E-mail System.

   The County's e-mail system is a communications system for operational purposes and generally not intended to be used as a records storage system.

2. Retaining E-mail Business Records.

   To the extent that e-mail messages constitute official business records to be retained pursuant to the County's records retention policy and records retention schedule, such e-mail messages shall be retained using one of the following methods.

   a. Save the message or output it to a PDF electronic file and store in an official electronic records storage repository.
   b. Print the message and store it in an official records storage filing system.

c. Emails that exceed the retention policy as outlined below are to be deleted from the local computers and shall not be stored or searchable on external USB devices.

Users are responsible to follow the County's records destruction procedure for retained email messages that are official business records when the records retention requirement has been met.

3. Retaining E-mail Pertaining to Litigation.

E-mail messages pertaining to an anticipated or actual legal action must be retained until the litigation is concluded regardless of the records retention requirements.

4. Deleting E-Mail Messages.

E-mail messages that do not serve a business purpose shall be routinely discarded. For that reason, each User has the same responsibility for their e-mail messages as they do for any document they obtain in the course of their official duties, and must decide which communications should be retained for business or legal reasons and which should be discarded. If a User has any questions regarding whether an e-mail should be retained as a business record, he or she should seek guidance from their supervisor and/or Department Head who may consult with the County Attorney's Office as necessary.

5. Automatic Deletion of Messages in inbox and subordinate folders created under the User account will be as follows; this includes sent items and deleted items folders. E-mail messages in Users' inbox folder will be automatically deleted based on defined rules and in compliance with the retention policy as early as 90 days from receipt or generation. E-mail messages in folders under the Users account will be automatically deleted based on defined rules as early as 2 years from receipt or generation. If a message constitutes an official business record that requires being retained pursuant to the County's records retention policy, the User should preserve the message as described above within 90 days.

6. Local E-Mail Archives Not Supported. The use or creation of local e-mail personal archive files (e.g.: Outlook.pst fries) are not supported. Such archive files are not backed up. Users shall not store official business records in .pst type files (e-mails} or on locations within the County's server infrastructure unless authorized by Department Head. Any storage of business e-mail records beyond defined rules shall be approved in writing by the Department Head for business operation purposes. All employees are to follow the Records Retention Policy as adopted by County Commissioners Court noted in the Records Management Policy that both District and County Clerk’s Office’s have copies for employees to reference and revised from time to time.

7. E-mail System Backups.

   The County's e-mail system is backed up to separate media regularly and stored offsite for disaster recovery purposes.

h. Internet

Access to the Internet exposes the County to external threats to its information systems and data. As such, the County takes precautions to protect itself from these threats using cyber-security systems and controlling and managing internet access.

a. Authorization

Users are provided internet access if authorized to use County Technology Resources as necessary for County business.

b. Internet Services Provided

The following internet services are provided for authorized Users.

- E-mail. Send *I* receive E-mail messages to *I* from external recipients *I* senders.
- Web Browsing. World-Wide-Web (WWW) services using the hypertext transfer protocol {HTTP or HTTPS - Secured) through web browser software (e.g.: Windows Edge or Google Chrome).

The following internet services are only allowed on an as-needed basis with business justification and IT Director approval.

- File Transfer Protocol (FTP, SFTP or FTPS – Secured). Send *I* receive files over the Internet to *I* from an FTP server. Business use examples include mandatory data reporting to the State or authorized data interchange with a business partner (e.g.: bank or service provider).
- Peer to Peer File Sharing {P2P). Peer to Peer file sharing allows one to download or upload files with others (nodes) on the Internet typically using torrents and P2P software. This service is not typically used for business purposes and is prohibited without a compelling business case.

i. Prohibited Websites

Intentional access to websites that promote or predominantly contain the following content are prohibited:

- Any website for which there is not a documentable business purpose to visit
- Obscene or sexually explicit content
- Illegal activities
- Violence or hate
- Online gambling and gaming
- Video streaming sites (except those approved by the County Commissioners Court as required for operational or business purposes, such as employee training videos.)

The County maintains the right to enable website content monitoring and filtering software that will block prohibited website access and monitor User browsing history. Regardless if website filtering is in place, Users should take care to avoid prohibited websites, or otherwise use the Internet for non-business purposes.

j. Network and Cybersecurity

1. Network Access

The County's computing environment is comprised of a common network that includes a collection of cabling, switches, routers, gateways, access points, servers, operating systems, databases, applications, and other technology resources. Access to the County computing environment is by way of a network User account (AKA network domain account or Active Directory (AD) account).

Users must receive authorization from their Department Head or designee, or sponsoring department contact to obtain a County network User account. The director or sponsoring department contact must submit a support ticket via the County's IT Helpdesk system requesting the needed access.

IT may revoke, or deny access to County Technology Resources without advance notice as required to ensure the security and integrity of the County's network and computing environment. The Department Head will be notified of network access violations.

2.Passwords

User accounts and passwords are used to secure access to network and computing resources. Passwords are the front line of protection for User accounts. A compromised User account can put County Technology Resources at risk. As such, the following rules and terms apply to **ALL** Users passwords.

3.Password Rules

a. Users shall use strong password(s) to access County Technology Resources. Unless other password rules exist for a given system, the following rules should be used when selecting a password.

- At least eight characters long
- Contain a mixture of at least 1 capital letter and 1 number. (example Welcome1)
- Must not contain the Username

b. It is suggested that passwords be created that can be easily remembered yet hard to guess. One way to do this is to create a password based on a song title, affirmation, or phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be something like "TmB1w2R!" or another variation.

c. Network User account passwords will expire at a set time interval {e.g.: 4 months). A Windows message will indicate pending password expiration when the expiration date is approaching and will provide a link to reset the password.

d. The last 5 passwords cannot be used when resetting a network User account password.

e. Network User accounts will become locked after 5 failed attempts with the wrong password. If this occurs, 2 options are presented; 1) Contact another employee and request that they input a helpdesk ticket requesting a password reset, or 2) wait 30 minutes for the automated system to clear and try your password again in the event of a locked account.

4. Password Protection

User account passwords are to be treated as sensitive and confidential.

a. Users are not to share passwords with anyone. This includes supervisors, support staff, and IT support personnel.

b. User passwords should not be written down unless placed in a locked location.

c. Passwords should not be sent in an e-mail or text message, or voicemail.

d. If a file is used to store passwords, the file should be encrypted and a strong password used.

e. Users who suspect their account or password has been compromised should change their password immediately and report the incident to their supervisor and IT staff.

f. Accounts are to be used only by the assigned authorized User of the account. Attempting to obtain another User's account password is prohibited.

k. Remote Access

1. Authorization

2. Remote access to the County's network over the Internet (Virtual Private Network - VPN) will be considered based on business-need on a case-by-case basis. A request for remote access must be authorized by the User's Department Head or designee. The following general criteria will be considered.

- County employees in management positions.
- County employees assigned with full-time IT support responsibilities.
- County employees assigned mobile computing devices to perform their specific job functions offsite during regular work hours.
- County employees assigned mobile computing devices and required to perform job functions outside of regular work hours.
- County employees under special circumstances authorized by Department Head and IT Director.
- Contractors, consultants, and vendors providing project specific services to the County such as IT support.

c. Non-exempt hourly employees are prohibited from accessing the County network and systems during off-duty hours unless pre-approved by the employee's supervisor. Non- exempt employees will be compensated for any approved overtime.

d. Information about the User's remote computing environment must be provided to IT staff as part of the remote access request. IT staff will review the information to assess the security risk for consideration in granting remote access.

e. IT support staff may remotely access a County-owned computer/device only after prior verbal notification to User.

l. Other Provisions

1. Aside from County-provided mobile devices, the remote User is responsible to provide, configure, and support the remote computer, software, and internet access. The County will provide the remote access client software or access to a *remote* access *web* server.
2. A remote User's computing environment must be on a supported operating system and include reputable anti-virus *I* malware software with up-to-date definitions.
3. Non-sensitive or non-confidential County data may be temporarily copied via remote access to a User's remote computer only to the extent necessary to fulfill

the designated job or service responsibilities of the User.

4. Remote Users shall not provide access to, share County data or printed reports to others except as authorized by their supervisor or assigned County contact. Remote Users shall protect County systems access, data, and printed reports from unauthorized access or disclosure. Proper protective measures include securing the remote computer and reports when unattended and shielding remote computer and reports from unauthorized viewing.
5. Remote User sessions will be automatically disconnected after a designated threshold of time of Inactivity. The User must then logon again to reconnect to the network.
6. Split tunneling is not permitted. Users will not be able to connect to another network, including one's own private network, while remotely connected to the County network.
7. Encryption beyond that provided by the County's remote access server is permitted only with prior approval of the Information Technology Director or designee.
8. Department supervisors or assigned department contacts shall immediately notify IT staff when the need for a User's remote access has ended.

m. Antivirus

IT will install and configure anti-virus *I* malware software on County-issued computers *I* devices. Anti-virus *I* malware software detects and prevents most viruses and malware from causing harm, *but it* is not perfect. *New* malware comes out often which constantly poses new threats.

Users shall not interfere with the anti-virus *I* malware software installed on their assigned computer *I* device.

Users shall immediately contact IT staff if they suspect their computer has been infected by a virus or malware. It is advised that if such occurs, User should immediately shut down the computer and or disconnect the computer from the network if possible.

n. Cybersecurity

The security of the County's Technology Resources is the responsibility of all Users. The County will provide mandated state-wide training for all employees to guard against malicious disruptions *or* inappropriate use that might subject the County to risk. All employees are required to complete the mandatory state Cybersecurity training along with any additional technology trainings as deemed necessary by the IT Director.

In the event that a County Technology Resource under a User's control is or appears to be compromised, the User must contact IT staff immediately and follow

instructions given by IT. In addition, the User should notify their supervisor or assigned County contact. IT after hours contact information should be posted at all locations of the County.

o. Computer Equipment and Software

The County will assign computer equipment and software to employee Users for the necessary performance of their job functions. The County may provide computer equipment and *I* or software to other classification of Users who provide services to the County (i.e.: contractors or vendors) as approved by the sponsoring User's department Head or designee and the IT Director.

a. Computer Equipment

Computer equipment includes items such as, but not limited to, personal computers (also referred to as desktop computers or workstations), laptops, storage, monitors, keyboards, mice, printers, plotters, scanners, speakers, cameras, and cables.

- Users are responsible to protect and properly care for their assigned computer equipment.
- Users shall use County computer equipment properly and not misuse it. Users should contact IT staff if they need assistance using any County computer equipment.
- Users should not use computer equipment assigned to another user.
- Users should always use their own network User account to login regardless of the computer *I* device being used.
- County-owned computer equipment may only be installed, changed, *or* removed by IT staff unless approved by IT Director.
- All County computer equipment must be purchased and approved through IT Department and approved by IT staff before the purchase. IT staff will review for system compatibility and charge to departments as appropriate.
- IT staff will coordinate the disposal of computer equipment. Computer equipment may have special disposal requirements and may contain confidential information that needs to be properly removed by IT staff.
- Additional provisions for laptops, tablets, and smartphones are in the Mobile Devices section.

p. Software

Software includes, but is not limited to, operating systems (e.g.: Microsoft Windows), Microsoft Office (e.g.: Word, Excel, PowerPoint, Access}, applications, anti-

virus and other utility software.

a. Software installed on or used through County Technology Resources must be approved by the IT Director prior to purchase. This includes client application software (sometimes referred to as "thick" or "faf' client software) or Software as a Service (SaaS}, also referred to as cloud-based application services.

b. All software used by Users on or through County Technology Resources must be properly licensed or the County must have legal right to use (e.g.: in-house developed).

c. Unauthorized use, copying, transfer, or reproduction of licensed software is prohibited and in violation of copyright laws. Copyright infringement can subject the User and County to liability for damages to the software manufacturer.

d. IT staff will maintain an inventory of County-owned software licenses. Upon acquisition, software licenses should be provided to IT. User manuals will be provided to and stored by department Users.

e. Software may only be installed, changed, or removed from County Technology Resources by IT staff unless otherwise approved by the IT Director.

f. Users are not permitted to interfere with anti-virus or anti-malware software installed on their assigned computer(s).

q. Mobile Devices

a. <u>Authorization</u>

Users must receive authorization by their Department Head or designee in order to access County Technology Resources using a mobile electronic device ("Mobile Device"). Additionally, mobile devices must be approved to access County Technology Resources by the department head and the IT Director.

b. <u>Personal Mobile Devices Approval and Usage</u>

A personal mobile device such as a cell phone may be authorized for access to County Technology Resources for County business during and after normal work hours if:

- In compliance with the County's Reimbursement Policy, Section regarding cell phones
- Users receives written authorization from their Department Head for operational consideration
- And IT Director approves for technical compatibility.

The following understanding and terms apply to using a personal mobile device for County business use.

1. An employee's work duties may require the use of a mobile device/cell phone during or after the work day. If the Department Head determines a mobile device is required to perform one's job duties, he or she may authorize the issuance of a County-owned mobile device to the employee or personal mobile device stipend.
2. Personally owned mobile devices are the responsibility of the employee and not supported by the County's IT staff.
3. The County may prohibit an employee from using his or her personal device to conduct County business at any time if determined by the Department Head to no longer be necessary for the employee's position.
4. Non-exempt hourly employees are prohibited from using their personal devices for County- business unless pre-approved by the employee's Department Head for an operational necessity. Non-exempt employees will be compensated for any approved overtime worked.
5. The use of personal devices to access County Technology Resources shall be subject to the County's technology control, policy and security.
6. Users have no reasonable expectation of privacy while using County Technology Resources from their personal mobile device such as network traffic, website access, and e-mail messages.
7. Users are responsible for their personal devices, including, but not limited to, the cost of the device, service plan, accessories, maintenance, repair, and any insurance or warranties.
8. The County is not responsible for damage to Users' personal devices including when being used for County business and accessing County Technology Resources.
9. A User is responsible for all activity performed from his or her mobile device when using the County's Technology Resources and will take all reasonable care to protect his/her device from unauthorized access, compromise, and to be free from malware.

r. <u>County-Owned Mobile Device Management</u>

County-owned mobile electronic devices will either be centrally managed by IT or managed by specific departments. Departments may manage inventory and software contracts for cell phones, radios, and other mobile electronic devices specific to department programs and services. IT centrally manages all County-owned mobile computer devices such as laptops, tablets, iPads, etc. In addition, IT is responsible for review of all County-owned mobile devices for system compatibilities and policies.

related to mobile electronic devices.

a. Users shall not attempt to bypass mobile security and management.

b. Authorized Users shall maintain data on a mobile electronic device in accordance with the County's Records Policy.

c. County information on County-owned mobile electronic devices may be subject to the Texas Public Information Act or any other Texas laws pertaining to public employees/officials. Users must comply with public records request related to County data on County mobile electronic devices.

d. IT may activate audit trails without notice for the purpose of identifying unusual usage patterns or suspicious activity to determine if the mobile device has been compromised or to identify misuse.

e. The County reserves the right to audit the configuration and content and inspect files stored on County-owned mobile devices without notice.

s. <u>Mobile Device Support</u>

1. County-Owned Mobile Devices

a. Support for County-owned mobile devices can be obtained through the issuer depending on the type of device (either the specific department or IT).

b. Requests for new mobile computer devices such as laptops or support for such devices should be submitted to the IT Help Desk and quotes will be provided by IT staff.

c. Users should not attempt to repair County-owned devices themselves.

d. IT will make best-effort attempts to fix problems Users experience on the County-owned mobile device. However, it may become necessary to reset a device to factory settings or wipe it to clear a problem. In such a case, IT will re-initialize the device for County business use. The County IT staff is not responsible for personal data or applications lost.

e. Mobile applications required to conduct County business must be approved by IT prior to installation.

f. Applications should be updated by downloading updates when prompted. It is recommended that mobile applications be updated to keep them running properly.

g. Departments are required to pay for mobile device repairs and *I* or replacements.

2. <u>Personal Mobile Devices</u>

a. An employee may be authorized to use their personal cell phone per the Reimbursement Policy. Authorized Users may use supported personal mobile

devices for accessing County e-mail and other authorized County Technology Resources.

b. IT will assist and advise employee in configuring the personal mobile device's County e- mail and other County Technology Resources as authorized in writing by each Department Head and the IT Director.

c. The User is responsible for their own device and application support from the manufacturer, service provider (ISP) or third-party. IT does **NOT** provide support services for Personal Mobile Devices.

t. Mobile Device Security

All mobile electronic devices shall be physically and electronically protected at all times. This includes, but is not limited to the following:

Physical Security (County-owned Devices)

1. Smart Phones should be equipped with a case to reduce risk of physical damage during a drop.

2. Mobile devices should not be left unattended in any public locations.

3. Mobile electronic devices shall not be left in vehicles in plain sight.

4. Physical security such as a laptop cable lock or a locked cabinet should be used when left unattended inwork areas.

Electronic Security

1. Users shall protect access to their mobile device with a strong password, PIN, or bio- metric (e.g.: fingerprint) security.

2. Users shall not disclose their passwords or PlN's to others.

3. Users shall employ up-to-date anti-virus or anti-malware software approved by IT on any client computers used to synchronize with mobile devices.

4. Users will not modify County-owned mobile devices without approval of IT.

5. IT may restrict the mobile device or User from accessing County Technology Resources.

6. The User shall not store County data to resources outside the County computing environment, such as Apple iCloud, Dropbox, Google Drive, Microsoft OneDrive, or other cloud-based file storage services without approval from IT.

7. Users should not use County-owned devices as Hotspots without approval by IT.

8. IT may remotely disable, wipe (erase), or reset County-owned mobile devices under the following circumstances:

a. Device is lost or stolen.

b. Device is replaced by another device or retired without replacement.

c. Device is transferred to another User.

d. User separates from the County (e.g. retirement, resignation, termination).

e. To repair a software issue (with knowledge of the User).

f. The device is infected by a virus or other malware.

g. To protect County Technology Resources.

h. Upon request of the User's Department Head or designee.

9. Department Head or designee will be notified of any County-owned mobile device alteration or policy violation.

+++++

u. Mobile Device Data

1. Wherever possible, data is to reside on the County's network rather than downloaded to the device.

2.Access to sensitive and/or confidential data on mobile devices must be made securely and with considerable care.

a. Encryption should be used.

b. Sensitive and/or confidential data should not be stored on mobile devices. Sensitive and/or confidential data may be temporarily downloaded for access, but the User should ensure that the downloaded data is removed from the device when finished accessing it.

c. Law Enforcement Data: Accessing SO, Department of Justice (DOJ), and other law enforcement systems criminal information and/or secondarily derived information via mobile devices is prohibited per the Texas Law Enforcement Telecommunication System (TLETS) ·Policies; Practices, and Procedures (PPP) and the Criminal Justice Information Services (CJIS} Security Policy unless the device uses FIPS 140-2 encryption and multi-factor authentication, or any access method or system already approved by Texas DOJ. Such access requires approval by SO Management and configuration by IT staff.

d. Any County business electronic communication, or information stored on a mobile device, County-owned or personal, may constitute a record subject to disclosure under the Texas Public Information Act (TPIA), the Texas Code of Civil Procedure, the Federal Rules of Civil Procedure, or other applicable statutes, regulations, or legal authorities. Users shall provide access and *I* or produce records that meet the requirements for public disclosure stored on the mobile

device upon the County's request.

e. Authorized Users and mobile devices may connect to the County's e-mail services. Other County services may be provided as authorized.

f. It is the User's responsibility to back-up any incidental personal data and applications on County-owned devices. Users of County-owned cell phones are prohibited from using the device for personal purposes. In the event a County-owned device needs to be wiped of all its data, all data and applications will be lost. The County bears no legal or financial responsibility for loss to personal data or applications.

v. Access and Disclosure

i. Users may have access to data and information ("Data") in County information technology systems through their system User account(s) and in the course of performing their job duties or service functions.

ii. Regardless of system access capability, Users shall not search or seek out Data in County systems, databases, repositories, and files except as necessary and required in the performance of their job duties or service functions.

iii. Users shall not share or disclose Data in County systems, databases, repositories, and files to others except as necessary and required in the performance of the User's job duties or service functions, and then only in a manner consistent with any other County policy or practice.

iv. Any disclosure should be in compliance with departmental policies and procedures and local, state, and federal laws.

v. Users should consult with their supervisor to obtain guidance if uncertain about sharing or disclosing Data.

w. Sensitive and Confidential Data and Information

1. Confidential Information is privileged information for a designated purpose that is only intended for recipients with a business need-to-know.
2. Disclosure of confidential data may violate local, state, and/or federal laws.
3. Users shall not access, take, copy, share or disclose sensitive and/or confidential Data without the authorization from their Department Head or designee which approval shall comply with any other pertinent County policy.

18. Data Storage and Backups

a. File Storage

Files should not be stored on User workstations, portable or mobile devices. These systems and devices are not backed up, and the information may be lost and can extend the legal liabilities of the County.

County information technology systems store Data on servers used to conduct County business. Data stored on production County-maintained servers are backed up nightly.

Users should store Data pertaining to County business on production County-maintained servers.

b. Sensitive and Confidential Data

1. Users shall not store archive emails, copy sensitive data and/or confidential information on external storage systems including removable media (e.g.: USB *I* Flash drives, SD memory cards, CD/DVDs) or cloud-based services (e.g.: Google Drive, iCloud, One Drive, Drop Box), unless authorized by their Department Head or

designee and the IT Director. If removable media is used, the device must be encrypted and password-protected. If removable media is lost or stolen, the loss should be reported immediately to the Department Head and IT Director. Placement of the information on the removable drive may be performed or enabled by IT staff if approved.

cWhen a storage device containing sensitive and/or confidential information needs to be disposed of (e.g.: retention expiration, retirement of hardware, no longer needed, etc.), it should be provided to the IT department for proper disposal. The disposal will involve the media be over-written at least three times using specialized software designed to permanently erase data, physical destruction (e.g.: crushing, shredding, incineration), or degaussing (magnetic destruction).

d. Data and Records Retention

1. Retention and Destruction

County records are subject to the County's Records Management Manual and Records Retention Schedule that is adopted by the County Commissioners Court and revised from time to time. All Users regardless of position within the County have access to these policies located in both the District and County Clerk's offices and they shall adhere to and comply with the Records Retention Schedule *I* Policies. Records are not to be destroyed without proper authorization and following the records destruction process required by the County's Clerks and County Attorney.

X. Telephones and Voicemail

Telephones and voicemail are provided at County offices and assigned to Users for the purpose of conducting County business communication.

Users shall be professional and responsible when using the County's telephone and voicemail systems.

Telephone calls are logged and may be reviewed by supervisors and/or Department Head.

Provisions for use of mobile phones or smart phones are identified in the Mobile Devices section of this policy.

y. Technology Purchases

Centralized information technology standards, architecture, processes and practices maximize the reliability, integrity, efficiency and performance of County Technology Resources. As such, the IT Director and staff are to be involved in all technology-related hardware and software purchases for County operations. This includes overview of hardware, software or SaaS Cloud Service contracts.

Departments are required to contact the County's IT Director prior to purchasing or entering into any agreement for information technology goods, services, or support. The IT Director reviews all information technology purchases to evaluate compatibility with the County's infrastructure.

Any purchases of technology products (hardware, software or SaaS applications) that are purchased prior to engaging the IT Director are considered standalone systems and will not be supported by IT and may not be allowed access to County Technology Resources .. For larger projects, the IT Director should be contacted early in the planning process.

Users may request computer hardware through the IT Help Desk. IT will review, recommend and approve appropriate requests based on standards, strategic direction, available resources, and ability to support.

Any technology equipment that has been replaced must be turned over to IT upon replacement. IT staff manages e-waste disposal, redistribution and reallocated of technology equipment to other Users as appropriate.IT maintains a technology asset inventory database and collaborates with Accounting on asset record keeping for the County.

20. Separation or Discontinuance of Service

The following provisions apply to Users who separate or discontinue service from the County:

a. The User shall return his or her county-assigned Technology and other Resources (e.g.: mobile devices, parking and building access cards) to his or her supervisor or assigned County contact before leaving the County. The User's supervisor shall then return the County Technology

Resource(s) to IT or make a request to IT to re-provision the Resource(s) to another User.

b. The User should forward any e-mails pertaining to County business from their personal e- mail account(s) to their supervisor or assigned County contact e-mail address.
c. The User shall return any County data files the User has on external media to their supervisor or assigned County contact.
d. The User's network and system accounts will be disabled after the separation date. A Department Head may request an alternative disable date to IT.
e. After separation date, the User should not attempt to access County Technology Resources even if resources appear accessible.

21. <u>Netiquette</u>

Users are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to, the following:

a. Be Polite. Never send, or, encourage others to send, abusive messages or communications.
b. Use Appropriate Language. Users are representatives of the County. A User may be alone with their computer, but what is written online or in e-mail can possibly be viewed publicly. Users should never swear, use vulgarities, or any other inappropriate language or communication online or in e-mail.
c. Privacy. Users should not reveal personal data online or in e-mail (e.g., home address, telephone number, etc.).
d. Disruptions. Users should not use County Technology Resources in a way that would disrupt or disturb others. Do not use loud computer sound; instead use a low volume when working near others. Silence mobile phones during meetings.
e. Be Brief and Concise. Long extraneous communication is not as effective.
f. Proof Read and Spell Check. It is a good idea to proof-read and spell-check messages before sending. Try to make communication easy to understand and to read.
g. Consider that humor and satire are very often misinterpreted and can be unprofessional.
h. Cite references for any facts presented.
I. Forgive the spelling and grammar errors of others.
j. All users are human beings. Don't "attack" correspondents; instead persuade with facts.

22. Violations

Violations of the County's Technology Use Policy may result in removal of access to County Technology Resources and *I* or be subject to disciplinary action, up to and including termination. In the case of illegal activity and *I* or malicious use, the County may refer the violation to law enforcement and *I* or the County Attorney for potential criminal investigation and prosecution and *I* or civil action