604 – ACCEPTABLE USE OF INFORMATION SYSTEMS

Section 604.01
Purpose

The purpose of this policy is to maximize the effective, efficient, and secure use of Fort Bend County information systems. The Information Technology Department (IT) has been designated by Commissioners Court to provide for the development, deployment, installation, repair, service, and security of the County's information systems. IT shall set forth approved standards, protocols, policy and procedures that must be followed by County officials and employees in order to prevent breaches of security, and to protect the County from liability, business interruptions, and service failures due to inappropriate use of computers and other information systems.

For purposes of this policy, information systems includes equipment and software such as computers, tablets, phones, servers, hard drives, thumb drives, files, cloud storage, other equipment and software which may be used to collect, record, process, display, and transmit information.

All software and hardware purchases must be approved and submitted by the Information Technology Department to ensure compatibility with and protection of County information systems.

All software and hardware purchases must be approved by the Information Technology Department to ensure compatibility with County information systems. County employees are not authorized to install hardware or software or otherwise make changes to County electronic systems. Installation of hardware and software is to be performed by the Information Technology Department.

Violation of any part of this policy may result in withdrawal of access to information systems and devices, and/or disciplinary action, up to and including termination of employment. Employees who have any questions regarding acceptable use of information systems should consult with their supervisor or contact the IT Service Desk.
.

Section 604.02
Authorized Access

Employees will be assigned access to the information systems that are necessary to perform job duties. Department Heads and Elected Officials will provide authorization to Information Technology for each employee's access. Department Heads and Elected Officials shall also request information systems equipment such as computers, mobile phones, and other devices deemed necessary for employees of their offices, and request such equipment from the IT Department via normal budget and procurement processes.

Employees are responsible for the proper use, care and security of all systems and devices they are entrusted to use in accordance with this acceptable use policy. All information systems and devices are the property of the County, not the individual employee. Access to systems and devices can be withdrawn at any time if an employee does not adhere to this policy.

Section 604.03
Acceptable Use

Improper use of County Information Systems could expose the County to risks, including malicious software, compromise of network systems and services, loss of property, exposure of

protected information and other legal liabilities. Therefore, the following activities are prohibited and engaging in such activities may result in disciplinary action, up to and including termination of employment. Note that this list is non-exhaustive.

1. Violations of rights of intellectual property, including, but not limited to, the installation or distribution of software products that are not appropriately licensed for use by Fort Bend County.
2. Unauthorized use of copyrighted material for which Fort Bend County or the end user does not have an active license.
3. Accessing user accounts, data, or information systems, for any purpose other than conducting County business, even if the user has authorized access.
4. Purposeful introduction of malicious programs into the County network or on information systems (i.e. worms, viruses, Trojans, etc.).
5. Revealing one's account password to others or allowing another individual to use one's account.
6. Purposely causing security breaches or disruptions of network communication.
7. Unauthorized port scanning or security scanning unless expressly permitted.
8. Intercepting data not intended for the employee's host unless this activity is part of the employee's normal job.
9. Circumventing user authentication or security of any information system.
10. Introducing honeypots or similar technology designed to lure cyber attackers and detect, deflect, or study hacking attempts to gain unauthorized access.
11. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, disable, or deny a user's access to an information system, via any means, locally or otherwise.
12. Altering the operation systems (i.e. jailbreaking) of County-issued devices.
13. Installation of unauthorized remote desktop software (i.e. TeamViewer, Chrome Remote Desktop).

(Note that some County employees, such as law enforcement or IT, may engage in above activities as part of their legitimate job duties, but only as authorized by the Department Head or Elected Official and the Director of Information Technology.)

Section 604.04 Public Accountability and Limited Right to Privacy

County employees are provided with information systems access and equipment in order to conduct assigned duties in service to the public. As custodians of resources entrusted to them by the public employees must be mindful of how to most appropriately utilize these resources. Personal use of County information systems should be minimal, and in no way interfere with productivity or interfere with information systems access for others. Employees can have no expectation of privacy for any information contained on

County information systems, including communications of a personal nature. The County has the right to view or monitor all activity conducted on County information systems. All information contained on county information systems may be subject to disclosure under the Public Information Act. Employees are prohibited from using County information systems for any of the following activities:

1. Using unprofessional, abusive, profane, or offensive language.
2. Expressing personal views about religion, politics, sexuality, or any other personal views not related to County business.
3. Using information systems to transmit fraudulent, libelous, or threatening information, or to engage in activities such as discrimination, harassment, degradation, or bullying of an individual or group of individuals in violation of Policy 201, Respectful Workplace.
4. Using information systems to conduct personal business for financial gain.
5. Using County information systems to campaign for public office.
6. Using information systems to engage in criminal activities, to gamble, to view, download or transmit pornography, or to engage in any other activity that would be a violation of County policies.

Section 604.05 Information Storage and Transmission

Information stored locally (e.g. hard drive or desktop) is not protected by routine backups and cannot be restored. Therefore all County data and work product should be stored on network drives to avoid loss or theft of data or interruption to business continuity. County data should not be saved on a personal cloud storage or any cloud storage service not approved and authorized by IT for County business. Departments are not authorized to establish new cloud services without permission from IT.

Sensitive information such as Protected Health Information (PHI) and Personally Identifying Information (PII) must be treated securely and may not be stored on computer hard drives unless the information is encrypted in compliance with Federal Information Processing Standards (FIPS) 197. Further, sensitive information should not be shared or transmitted to parties outside the County network via email, fax, instant messaging, text message, or voicemail without appropriate controls that include encryption, authentication of recipients, and appropriate designation as confidential or sensitive.

Section 604.06 Email

Only County-provided email accounts shall be used to conduct Fort Bend County business. County provided email accounts should not be used to send or receive non-business related emails. Use of third-party email services, such as Gmail or Yahoo, including the auto-forwarding of County email to outside email services to conduct County business, is prohibited.

Employees should include a Privacy or Confidentiality Statement on any email that may contain confidential or sensitive information. Emails containing sensitive or confidential information such as PHI or PII, should not be transmitted outside the organization without proper security measures as discussed in the section above.

Due to the sensitivity of emails, a new County email address will be created for employees that transfer to new positions outside their departments. The email address is property of the County and belongs to the position.

Emails sent or received by users while conducting County business are considered Fort Bend County records, and are therefore subject to records retention, open records, and security requirements.

Section 604.07 Protection of County Issued Devices

County information systems devices and equipment are the property of the County and not the assigned user. The user is responsible for the safety and security of all equipment they are entrusted to use. The replacement cost of a lost, stolen, or damaged device shall be charged to the budget of the user's department. An assessment of the circumstances leading to the loss, theft, or damage of the device may be conducted by Risk Management, Human Resources, IT and the department head or elected official, to determine if an employee shall be responsible for all or a portion of the cost of the device.

Employees should follow these minimal best practices to protect all County devices, including mobile devices:

1. Keep liquids and caustics away from devices, and place devices in stable and secure locations.
2. Keep devices away from children and pets and do not allow others to use the device.
3. Make note of the device's make and serial number that may be needed in the event a police report is needed.
4. Keep mobile devices in your personal possession whenever possible, or leave in a secure location.
5. If devices must be left in a vehicle, they should be locked in a trunk, glove box, or otherwise completely hidden from view.
6. Do not place County issued devices in checked luggage when traveling.
7. When passing a device through an airport or other security screening area, care should be taken to keep an eye on the device as best as possible while complying with the security procedures. Be sure to retrieve the device after screening!
8. As mentioned in the Storage and Transmission section, all data, especially sensitive data, should be stored on County network drives and not on the device hard drive!
9. Access to all County devices must be secured with passwords, dual authentication, Face or Touch ID, etc. and employees must not disable or attempt to bypass these security measures.

Mobile Device Management (MDM) software will be installed on all County owned mobile devices to ensure compliance and access to County information are properly maintained. All County provided mobile devices are subject to inventory, review and management by the Fort Bend County Information Technology Department.

In the event of a lost, stolen or damaged device, employees should immediately notify their supervisor and the IT Department. A Risk Management Incident Report must be filed. A police report must be filed for any lost or stolen County device.

If a replacement County cell phone has been requested (damaged or upgrade), the currently assigned County cell phone must be returned to IT before the employee can receive a new cell phone. County cell phones and associated cell phone number belong to the County and are not intended for personal use. As such, County cell phones and phone number cannot be "transferred" if the employee leaves the County, changes departments, or transfers to a position where the cell phone is no longer required. Rather, County cell phones (and power cords, etc.) should be returned to IT. The cell phone will be wiped and assigned to another County employee.

Employees will be required to pay for the replacement of a lost, stolen or damaged hardware token used for dual authentication (such as Yubikeys),

Section 604.08 Passwords and User Accounts

Unauthorized access or allowing unauthorized users to access County information systems is prohibited. Any form of tampering to gain unauthorized access to information systems is prohibited.

Password requirements will be established by IT and made available to all employees and new employees at Orientation. The requirements will be available on eConnect, and can be obtained from the IT Service Desk. All employees must adhere to the password requirements including use of strong passwords, changing passwords within an established timeframe, and not sharing their password with anyone, including a system administrator.

Employees with local administrative privileges on County devices should recognize the inherent responsibilities and increased risks. These include the potential loss of data, compliance with copyright laws and increased threat of compromise. Local Administrative rights should be managed with caution.

Accounts inactive for 21 days will be reviewed by IT to possibly be disabled. Accounts inactive for 90 days will be disabled by IT.

When using the account, a session idle for more than 15 minutes due to inactivity, will require the user to re-authenticate.

Section 604.09 Other Restrictions and Limitation on Use

To further ensure the appropriate use of County information systems, employees should note the following restrictions and limitations:

- Bring Your Own Device (BYOD): The use of a Personal Owned Device (POD) to access County network and resources. Personal Owned Devices include but are not limited to smartphones, personal computers, tablets, or USB drives. PODs are not allowed on the County network and are not to be used to host, access, or in any way come in contact with County data and systems unless approved by the IT Department.
- County employees may request to use their personal owned mobile device, such as a mobile phone, to access the County's primary wireless network, to access email directly from the County server, or to interact with other County equipment. If so, Mobile Device Management (MDM) software will be installed on the device to ensure compliance with access to County information systems. The mobile device must meet software compliance requirements set forth by the IT Department, or access will be denied.
- MDM software will allow the IT Department to remove all County information stored on a personal mobile device, if necessary, without accessing or interfering with the employee's personal information and applications on the device.
- If an employee owned mobile device is lost or stolen, the employee must immediately notify his or her supervisor and the Information Technology service desk so that appropriate steps can be taken to protect County information systems.
- Upon separation of employment, all County information will be remotely removed from the mobile device. The employee's personal data and applications are protected from this removal.
- Personal Owned Devices are allowed to access the County guest wireless network. Activities on the guest network are monitored and inspected. If a data breach, virus, or some other threat to the security of County data or technology structure is detected, the device will not be allowed to access the guest network. Personal Owned Devices including, but not limited to, iPads or iPods, PDAs, tablets, BlackBerry devices, mobile phones or cameras, shall not be connected to the County network infrastructure in any manner without proper approval. These devices should not be connected to County systems for purposes of charging power, transferring personal audio, video, or images as non-County owned electronic devices may introduce unnecessary risk to County systems and data.
- Internet of Things (IoT) Devices: The use of IoT devices (e.g., Google Nest devices, Alexa devices) on the County network must be approved by IT before connecting.
- Removable Media: Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. Personally owned removable

media devices are not allowed on County network unless approved by County IT. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players, mobile phones and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks

- Removable media devices must meet compliance with County security policies. Any devices not approved by IT, not in compliance, or are found to represent any threat to the County network or data will not be allowed to connect to a County device or the network.
- County Virtual Private Network (VPN): County VPN is not to be used on non-County devices. Third-party VPN usage is strictly prohibited.

Section 604.10 Annual Cyber Security Training

Texas Government Code Section 2054.5191 requires state and local governments to deny access to information systems to any employee or official who fails to complete a certified Cybersecurity training program on an annual basis. Each year, Information Technology will identify the certified training course to be taken, and advise employees and officials of the deadline to complete such training. It is the responsibility of each employee and elected or appointed official of the County to complete all required elements of the training.

Failure to comply with the training requirement will result in denial of access to County information systems, and could result in disciplinary action, up to and including termination of employment. Employees should direct any questions regarding the training to the supervisor or the Information Technology Service Desk.

Section 604.11 Separation of Employment

An employee who ends employment with the County for any reason shall be denied further access to County information systems. Employees must return any County issued information system devices they may have, including cell phones, tablets, laptops, desktops, flash drives, hardware tokens, etc., on or before the last day of employment. If the employee is unable to return County devices on or before the last day of employment, they may be allowed no more than two business days to return the devices. Until the devices are returned, the employee is responsible for the safekeeping of these County assets. The County shall take any measures available to ensure the return of the devices and the security of any County information contained therein.

Policy Approved and Adopted by:
Fort Bend County Commissioners Court
October 14, 1997
Revised: May 2, 2006
Revised: February 24, 2009
Revised: November 24, 2015
Revised: June 7, 2022