THE STATE OF TEXAS
FORT BEND COUNTY

Fort Bend County

ACCEPTABLE USE AGREEMENT

Document Version: v1.0

Change Record

DATE	VERSION	AUTHOR	CHANGES MADE
8/25/2021	0.1	CyberDefenses	Initial Draft
9/2/2021	0.2	CyberDefenses	Edits and additions
9/3/2021	0.3	CyberDefenses	Edit Changes
9/21/2021	0.4	CyberDefenses	Added Personal Own Device and Removable Media
9/28/2021	0.5	Russell Hill	Added Email Transmission of PHI & PII, and updated Storage to Include FIPS 197 compliance
10/8/2021	0.6	Emmanuel	Additions, Definitions, and Edits
10/14/2021	0.7	Russell Hill	Changed Travelling with… to County-Issued devices. Minor edits and additions.
3/31/20201	0.8	Emmanuel	Added replacement and lost devices policy

Table of Contents

Overview

This policy defines a level of acceptable performance and expectation of behavior and activity for Fort Bend County Employees who use County Information Systems. The rules in this Policy are in place to protect County employees and County information systems. Inappropriate use exposes County information systems to risks including malicious software, compromise of network systems and services, and legal issues.

Exceptions to the Acceptable Use Agreement need to be submitted to the Information Technology Service Desk for review and approval.

Scope

Anyone using a County device is bound by this Acceptable Use Agreement.

Definitions

Cloud storage - Is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. Examples include Apple iCloud, Dropbox, google drive, OneDrive.

Honeypots - A honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access.

Protected Health Information - As defined by the HIPAA Privacy Rule, protected health information (PHI) is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, transmitted, or maintained by a HIPAA-covered entity or its business associate in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. Examples include patient names, addresses, dates (including birth, discharge, admittance, and death dates), telephone and fax numbers, email addresses, social security numbers, driver’s License information, medical record numbers, Account numbers.

Personally Identifiable Information - Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Examples include a full name, employee ID, Social Security number, driver's license number, bank account number, passport number, and email address.

Information system - The equipment and software such as files, computers, tablets, servers, hard drives, removable thumb drives, cloud storage, etc. used to collect, record, process, display, and transmit information.

Intellectual property - Ideas for which property rights are recognized under patent, trademark, or copyright law. Usually a work originating from thought or an idea that is distinct, separate, clearly definable, and novel. Examples of intellectual property include designs, concepts, software, inventions, trade secrets, formulas and brand names, as well as works of art.

Jailbreak – Is the act removing a restricted mode of operation in a computer system or device that were deliberately placed there for security, administrative, or marketing reasons. For example, jailbreaking may enable content with digital rights to be used on any computer, or it may allow enhanced third-party operating systems or applications to be used on a mobile device.

Local storage - Storage that is physically local to the workstation or server.

Network - All associated equipment and media creating electronic transmission between any information system(s), such as wired, optical, wireless, IP, synchronous serial, telephony, etc.

Script - A computer script is a list of commands that are executed by a certain program or scripting engine. Scripts may be used to automate processes on a local computer or to generate Web pages on the Web.

Remote desktop software - Software that is used to access a desktop or desktop interface of a remote computer locally. It allows someone take control of another user's computer in a distant location.

Federal Information Processing Standards (FIPS) 197 - Is a standard that created the Advanced Encryption Standard, which is a publicly accessible cipher approved by the National Security Agency (NSA) for sensitive information.

County Devices - By no means exhaustive, include desktops, laptops, tablets, hardware tokens, cell phones, printers, etc.

Policies

Unacceptable Use

The following activities are, in general, prohibited. County employees may be exempted from certain restrictions while doing their legitimate job responsibilities.

Under no circumstances is any individual utilizing Fort Bend County information systems authorized to engage in any activity that is illegal under local, state, federal or international law.

The list of activities that follows is by no means exhaustive but rather serves to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the 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 (e.g., viruses, worms, trojans, etc.)

5. Revealing your account password to others or allowing use of your account by others.
6. Using an information system to actively engage in activities in violation of sexual harassment or hostile workplace laws.
7. Purposefully effecting security breaches or disruptions of network communication.
8. Unauthorized port scanning or security scanning unless expressly permitted.
9. Intercepting data not intended for the employee’s host unless this activity is a part of the employee’s normal job.
10. Circumventing user authentication or security of any information system.
11. Introducing honeypots, or similar technology on the network.
12. 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.
13. Gambling on Fort Bend County owned computers/devices is strictly prohibited.
14. Altering the operation systems (i.e., jailbreaking) of County-issued devices.
15. Installation of unauthorized remote desktop software (i.e., TeamViewer, Chrome Remote Desktop.)

Information Storage and Transmission

Sensitive information (i.e., PHI and PII) should be stored only on the County drives. Sensitive information may not be stored on computer hard drives without encryption compliant with FIPS 197 standards, nor may it be shared or transmitted to parties outside the County network via email, fax, Teams messages, text messages, or voicemail without appropriate security controls.

Controls should include encryption of messages and authentication of recipients (e.g., password protection of files; verification of fax numbers; cover sheets; marking documents as confidential).

Information stored locally on the computer are not backed up. Information should be stored on the County drives, home or department drive. Should a computer become inoperable, local files cannot be restored. County business should not be stored on Personal Cloud Storage, employees may only use cloud storage services approved and authorized by IT for County business. Departments are not authorized to establish new cloud services without permission from IT.

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. As custodians of resources entrusted to them by the public, employees should be mindful of how to most appropriately utilize these resources to perform their duties. Use of third-party email services (such as Gmail or Yahoo), including the auto-forwarding of Fort Bend County email to outside email services to conduct County business is prohibited.

Emails containing sensitive or confidential information such as Protected Health Information (PHI) or Personally Identifiable Information (PII) should never be shared or transmitted outside the organization without encryption through the use of a secure messaging system. It's recommended to use a privacy statement in each email containing sensitive information sent outside the organization.

Due to the sensitivity of emails, a new County email addresses will be created for personnel that transfer to new positions outside their departments. (The email 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 data and are subject to Fort Bend County records retention and security requirements.

Social Media

All Fort Bend County social media platforms shall be submitted for approval by the head of the requesting department or elected official. All Fort Bend County social media platforms shall be approved by County Judge's Office, and the Chief Information Officer. All content must be published using County approved tools. All content must be approved by the head of the requesting department or elected official, or designee, before posting. For more details on the County social media policy, please review the Employee Information Manual section 615.

County-Issued Devices

County-issued devices are always to remain under your physical control. At airport security checkpoints, set County-issued devices on conveyor belts only after the belongings of the person ahead of you have cleared the scanner. If you are delayed, keep your eye on the devices until you can pick them up. Do not place County-issued devices in checked luggage. If you must leave a County-issued device in a car, lock the device in the trunk so that it is out of sight. When travelling and taking County devices employees should note the make and Serial Number of the devices.

Employees are responsible for loss/replacement of County devices depending on circumstances (careless use, neglect, etc.). Lost or stolen County devices must have a police/incident report to file with Risk Management (Serial/Tag# required on the report). Employees who lose their hardware token will be required to pay for replacements.

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 a lost or damaged 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 their 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 changes positions (to where the cell phone is no longer required). Rather, County cell phones (and power cords, etc.) should be returned to IT in these cases. The cell phone will be wiped and assigned to another County employee.

County Virtual Private Network (VPN)

County VPN is not to be used on non-County devices. Third-party VPN usage is strictly prohibited.

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.

User Accounts

Employees are responsible for safeguarding their system access login and password credentials and must comply with the password parameters and standards identified in the County password policy found in the Employee Information Manual section 604.12. Passwords should not be shared, nor should they be provided to anyone, including system administrators.

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 not be taken advantage and 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.

All authorized users are required to take and pass Cybersecurity Awareness training as mandated by HB 3834. Network access will be suspended for users who do not complete training.

Bring Your Own Device (BYOD)

Bring-Your-Own-Device is the use of employee-owned devices to access County network and resources. BYOD devices include but are not limited to smartphones, personal computers, tablets, or USB drives. BYOD devices 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 County IT.

BYOD devices are allowed to access the County guest network but should not be plugged into any County-owned device. Fort Bend County IT support is not offered on these devices. Activities are monitored and inspected while on the County guest network. If IT detects a data breach, virus, or some other threat to the security of County data or technology infrastructure the device will not be allowed to connect to the County guest network.

Personal Own Devices (POD)

Users shall not connect personally owned, or other non-County owned, equipment or devices, including, but not limited to, USB or other storage or memory devices, iPads or iPods, PDAs, tablets, BlackBerry devices, mobile phones or cameras, 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.

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.

Related Standards, Policies, and Processes

These policies can be found on eConnect:

- County Password Policy
- Information Security Policy
- Information Security Standards