HUMAN RESOURCES DEPARTMENT
FORT BEND COUNTY, TEXAS

Kent M. Edwards, PHR
Director of Human Resources

To: Judge Robert Hebert
Commissioner Richard Morrison
Commissioner Grady Prestage
Commissioner Andy Meyers
Commissioner James Patterson

From: Kathy Novosad, PHR
Sr. Human Resources Generalist

Copy: Ray Webb, Director of Information Technology
Clay Elliott, IT Operations Manager

Date: November 18, 2015

Subject: Revisions to Employee Information Manual:
Policy 604: Electronic Systems Policy and Guidelines

Human Resources is submitting the attached revisions to the Employee Information Manual *Policy 604: Electronic Systems Policy and Guidelines*. The revisions were requested by the Information Technology Department, and reflect changes to increase security for the use of mobile devices that access County networks. In addition, to enhance system security, the policy includes new requirements for user passwords when accessing County networks. The attached document, "Password Requirements," will be placed on the intranet and updated as needed to reflect best practices in password security.

If you have any questions regarding the attached revisions, please contact Ray Webb or Clay Elliott in Information Technology.

301 Jackson Street, Suite 243, Richmond, TX 77469 * 281-341-8631 * Fax 281-341-8615
Kent.Edwards@co.fort-bend.tx.us www.co.fort-bend.tx.us

604 – ELECTRONIC SYSTEMS POLICY AND GUIDELINES

Section 604.01 Purpose

The purpose of this policy is to maximize the effective and efficient use of Fort Bend County electronic systems, to prevent breaches of system security, and to protect all employees of the County from liability and business interruptions due to inappropriate use of computers and other electronic systems. This policy cannot provide guidelines for every possible situation. Instead, it expresses the County's philosophy and sets forth general principles for the use of electronic systems by all County departments and offices.

The Information Technology Department will provide employees with access to electronic systems on an as needed basis with the authorization of the employee's Elected Official/Department Head. All electronic systems remain the sole property of the County, and not the individual user.

Section 604.02 Definition

For purposes of this policy, electronic systems are defined as all electronic equipment, media, and services including but not limited to, computers, telephones, cellular phones, voicemail, fax machines, copiers, radios, wireless devices, mobile devices and on-line services.

Section 604.03 Software/Hardware Purchases and Installation

All software and hardware purchases must be approved by the Information Technology Department, meet pre-established quality requirements, be compatible with other County electronic system's software and hardware and meet standard communications minimum requirements.

All installations will be performed by the Information Technology Department. Installing software, hardware or otherwise making changes to County electronic systems without written authorization from the Information Technology Department is prohibited.

To prevent accidental introduction of viruses or other harmful programs, employees may not install or connect any personal equipment, devices or software to County electronic systems without authorization from the Information Technology department. Prior to loading or downloading any information or software, the program must be scanned with a County approved virus detection program. If you identify a virus, worm or Trojan horse, or what you suspect to be one, do not attempt to fix the problem. Immediately turn your computer off, make notes as to what you observed, and contact the Information Technology Department.

Section 604.04 Copyright Materials and Issues

Employees should observe all copyright laws and license agreements pertaining to any County electronic system, software, or any information or material contained in on-line services. Violation of copyright laws or license agreements may result in disciplinary action, up to and including termination of employment.

Section 604.05 Access to On-Line Services

On-line services include but are not limited to e-mail, Internet and Intranet that Fort Bend County provides to employees. Access will be granted on an as-needed basis and as authorized by the Elected

Official/Department Head. Form 6A at the end of this policy should be properly completed and submitted to the Information Technology department to obtain access.

Section 604.06 Use of On-Line Services

The primary purpose of e-mail, Internet and Intranet is to facilitate County business. Every employee has a responsibility to use these services in a productive manner. All electronic transmissions, whether originated at or sent to the County, and all information obtained via the internet and intranet, shall be considered the sole property of the County and not the individual user.

If Fort Bend County electronic systems are used for personal purposes, this practice must be limited and must in no way interfere with an employee's productivity or work responsibilities. Even personal e-mail and Internet and Intranet use on County electronic systems may be subject to open records requests or subpoenas that could result in disclosure to the public of the content of the e-mail communications and/or the nature of internet/intranet use.

Section 604.07 Mobile Devices

County owned ~~M~~mobile devices include but are not limited to cell phones, ~~Blackberry devices,~~ Smart Phones, lap top, notebook or tablet PCs, Flash Drives, and MP 3 players~~, and Personal Digital Assistants (PDA).~~ Employees may be assigned County owned mobile devices if authorized by their elected official or department head. Such devices create additional security risks and operating expense for the County, and are therefore subject to the ~~following~~ provisions of this section. ~~:~~

Additionally, some County employees may choose to use their employee owned mobile devices to access the County's primary wireless network, access internal applications, to receive email directly from the County's server, or to interact with other County equipment. Use of personal mobile devices in this manner also create security risks for the County and for that reason require safeguards.

Therefore, Mobile Device Management software will be used to protect County assets and information for all mobile devices that access County resources, regardless of ownership. There is no intent nor will any action be taken to view, capture or track personal information on personal devices. The County data and information is stored and administered separately from personal data through the use of the MDM tool.

Provisions for County Owned Mobile Devices

1. Mobile Device Management software will be installed on all County owned mobile devices to ensure compliance and access to County information are properly maintained.

2. Employees are prohibited from installing unapproved and unauthorized software on county-provided mobile devices that could alter the operating system or disable the built in security features of the device. Employees should refrain from downloading additional software and services to county-provided mobile devices.

3. Fort Bend County Information Technology Department and

Fort Bend County Purchasing Department will publish and maintain a list of supported, approved mobile devices. As Information Technology equipment, final approval of such devices will rest with the Director of Information Technology.

4. Employees issued county-provided mobile devices are responsible for the security and safekeeping of those devices. Mobile devices must be returned to the County upon termination of employment.

5. No sensitive or confidential information should be locally stored on mobile devices. In the event that a mobile device is lost, stolen or misplaced, the Fort Bend County Information Technology department and the employee's department supervisor should be notified immediately so that appropriate steps can be taken to protect County assets.

6. All County provided mobile devices are subject to inventory, review and management by the Fort Bend County Information Technology department.

Provisions for employee owned mobile devices:

1. Employee owned devices may be utilized to gain access to internal applications and email if authorized by their elected official or department head. These devices include but are not limited to cell phones, Smart Phones, laptop, notebook or tablet PCs, Flash Drives, and MP 3 players.

2. Mobile Device Management (MDM) software will be installed on the employee owned device to ensure compliance and access to County information through the county's primary wireless network are properly maintained if the employee owned mobile device is used to access the County's primary wireless network, access internal applications, receive email directly from the County's server or interact with any county equipment.

3. The MDM tool allows for a separation of county data and personal data through policies that prevent data collection from personal email, content, or applications on the employee owned device. Personal information, cellular use, GPS, and telecom data all remain private.

4. The employee owned device must meet software compliance requirements set forth by the Information Technology department. Any device that has altered the operating system or disabled the security features of the device will be denied access to the county wireless network and email.

5. The Information Technology department with place a confidential security code on the mobile device which will be instituted for the MDM tool. This will allow secure connectivity to the Fort Bend County infrastructure without placing restrictions on the employee owned device. However, the security code will not be given to the employee and will be

maintained only by the Information Technology department.

6. No employee may connect, dock or otherwise synchronize any non-county mobile device, with any county computer, laptop, server, system or network without first installing the MDM tool on their device.

7. In the event that the employee owned mobile device is lost, stolen or misplaced, the Fort Bend County Information Technology department and the employee's department supervisor should be notified immediately so that appropriate steps can be taken to protect County information.

8. Upon termination of employment all Fort Bend County information will be remotely removed from the mobile device. The employee's personal data and applications are protected from this information removal.

The Information Technology department may terminate system access without warning or without further approval for any employee owned mobile device if the in the judgement of the Director such termination is necessary to protect the security of the County IT system.

For more information and definitions of mobile devices, please contact the Information Technology department.

~~1. Employees are prohibited from installing unapproved and unauthorized software on county-provided mobile devices. Employees shall refrain from downloading additional software and services, including but not limited to distinctive ring tones, games and other messaging services, to county-provided mobile devices.~~

~~2. Fort Bend County Information Technology Department and Fort Bend County Purchasing Department will publish and maintain a list of supported, approved mobile devices. As Information Technology equipment, final approval of such devices will rest with the Director of Information Technology.~~

~~3. No employee may connect, dock or otherwise synchronize any non-county mobile device, with any county computer, laptop, server, system or network without prior authorization from IT.~~

~~4.~~

~~5. Employees issued county-provided mobile devices are responsible for the security and safekeeping of those devices. Employees are expected to keep the devices in their possession at all times when on duty or on call. Mobile devices must be returned to the County upon termination of employment.~~

~~6.~~

~~7. No sensitive or confidential information shall be stored on mobile devices at any time. In the event that a mobile device is lost, stolen or misplaced, the Fort Bend County Information Technology department should be notified immediately so that~~

~~appropriate steps can be taken to protect County assets.~~

~~8. All County provided mobile devices are subject to inventory, review and management by the Fort Bend County Information Technology department.~~

Section 604.08 Illegal or Inappropriate Material and Prohibited Activities

Employees are responsible for the content of all text, audio or images that they access, place or send over the County's electronic systems, and for any equipment entrusted to their use. Messages sent via the Fort Bend County e-mail, Internet and Intranet systems are statements that may be attributed to the County. Therefore, Fort Bend County electronic systems may not be used to transmit, print, request, store, access or disseminate the following types of information:

- Personal views about religion, politics, sexuality, or any other subject of a personal nature;
- Fraudulent, libelous, harassing, threatening, discriminatory, sexually explicit, or obscene information, messages and/or material;
- Harassing, derogatory or inflammatory messages or remarks about race, age, gender, disability, religion, national origin, physical attributes or sexual preference;
- Abusive, profane or offensive language;
- Political issues or campaign-related material or information except as required by federal and state statutes for official County election-related business;
- Commercial, profit-making or private business activities;
- Unsolicited information regarding religion or politics
- Unsolicited information such as "Chain Letters" or spam.

Employees may not use Fort Bend County electronic systems for any of the following activities:

- Except in limited law enforcement investigations, no e-mail or other electronic communications may be sent which hide the identity of the sender or represent the sender as someone else or someone from another department or entity;
- Use of electronic systems in a manner that is likely to cause network congestions or significantly hamper the ability of others to access and use the services or equipment is prohibited. This includes but is not limited to the following items: Weather Bug, Internet Radio Stations/Sites, MP3 Files, Music/movie downloads;
- Introducing, creating or using software designed to destroy or corrupt the County's electronic systems in any way is prohibited. Destruction, theft, alteration, or any other form of

sabotage of County computers, programs, files, or data is prohibited, will be investigated and may result in discipline up to and including termination of employment and prosecution to the fullest extent of the law.

An employee who receives an inappropriate or illegal communication, or is aware of misuse of any electronic system, must promptly notify their immediate supervisor.

Section 604.09 Monitoring

THERE SHALL BE NO EXPECTATION OF PERSONAL PRIVACY OR CONFIDENTIALITY IN THE USE OF ANY FORT BEND COUNTY ELECTRONIC SYSTEM, INCLUDING ON-LINE SERVICES AND MOBILE DEVICES.

Electronic activities are to be treated as public information unless exempted by federal or state law. The Information Technology Department is authorized to conduct random software license audits and random monitoring of electronic activities. Any inappropriate use or excessive use of electronic systems for non-job related purposes will be reported to the appropriate County personnel, and the offending employee may be subject to discipline up to and including termination of employment.

Section 604.10 Single Point of Entry

Access to County and Library electronic systems is through the County's registered domain name(s) and each County department or organization is defined as a sub area within the official domain. If a specific domain name is required for a County department or organization, a request must be submitted to the Information Technology Department for review and recommendation to Commissioners Court.

Section 604.11 Filtering Services

Fort Bend County uses filtering services to monitor and/or block access to inappropriate site(s) on the Internet. The purpose of filtering is to protect County resources, conserve bandwidth and help enforce on-line service policies.

Access to certain blocked sites on the Internet and Intranet may be granted to employees who demonstrate a job necessity for such access. Department Heads/Elected Officials may submit a written request for access to the Information Technology Department.

Section 604.12 Passwords and Unauthorized Access

Unauthorized access or allowing unauthorized users to access County electronic systems is prohibited. Any form of tampering, including snooping and hacking, to gain unauthorized access to electronic systems may result in disciplinary action up to and including termination of employment.

~~Employees will be held responsible for misuse and unauthorized use of any electronic system entrusted to them.~~ To ensure protection of the security of the County network, protect data integrity, and protect County computer systems, all employees that have access to Fort Bend County computer systems must adhere to the password requirements as set forth by the Information Technology Department.

The password requirements are designed to protect the organizational resources on the network by requiring the use of strong passwords,

protection of these passwords, and establishing a maximum time between changes to passwords. The requirements apply to any and all personnel who have any form of computer account requiring a password on the organization network, including but not limited to a computer login account and e-mail account.

The password requirements shall be distributed to all employees and to all new hires during new employee orientation. The requirements shall also be readily available on the County intranet or by contacting the Information Technology Department Service Desk at ITServiceDesk@fortbendcountytx.gov, or 281-341-4580. A hard copy will be furnished on request. All employees are responsible for adhering to the requirements of this policy and the requirements set forth by Information Technology, and failure to do so could result in revocation of computer access privileges.

~~should take reasonable steps to guard system user IDs and passwords and otherwise protect County equipment.~~

Section 604.13 Remote Access

Remote access (employees who utilize modems from their desktops) is subject to the same electronic system guidelines.

Section 604.14 Storage

Information stored on any County electronic system will be retained in accordance with federal or state laws and policies established by Fort Bend County, whichever is greater.

Employees should not store information (*including but not limited to the items listed in Section 604.08*) on County electronic systems in a manner that is likely to cause network congestions or significantly hamper the ability of others to access and use the services or equipment.

Section 604.15 Termination or Separation of Employment

All County electronic system information and equipment is considered County property. Employees who terminate employment for any reason must return any County owned data and equipment with any information necessary for the County to continue using the electronic system uninterrupted. The following activities are prohibited and may be prosecuted to the fullest extent of the law:

- Accessing County electronic systems after termination of employment
- Providing third parties, or anyone else, access to County electronic systems
- Removing, copying or deleting data
- Failure to return computer files, data, programs, or other electronic equipment, including mobile devices

Section 604.16 Violation of Policy

An employee who violates any provision of this policy is subject to disciplinary action, up to and including termination of employment.

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

INFORMATION TECHNOLOGY DEPARTMENT

FORT BEND COUNTY, TEXAS

To: Fort Bend County
Attn: Information Technology Department
Fax #: 281/341-4526

REQUEST FOR INTERNET/INTRANET ACCESS

Date of Request: _____

Requestor's Name: _____ **Phone #:** _____

Requestor's Title: _____

Department: _____ **Dept #:** _____

Selected Applicant: _____

Applicant's Phone #: _____

Job Posting #: _____ **Job Title:** _____

Status: Full-Time ☐ Part-Time ☐ **Anticipated Start Date:** _____

Is current application on file at Human Resources? Yes ☐ No ☐

_____ _____

Elected Official/Department Head Approval **Date**

The following information is considered necessary in order to perform an evaluation of required access:

Primary Job Duties In which applicant will Need access to Internet And/or Intranet	_____
	_____
Other?	_____

For ITD Use Only:

Date of receipt of Applications: _____

Approval/Non-Approval: _____

Confirmed with Department: _____

PASSWORD REQUIREMENTS

Overview

As stated in Section 604.12 of the Electronic Systems Policy and Guidelines in the Employee Information Manual, all employees and personnel that have access to Fort Bend County electronic systems must adhere to the password requirements defined below in order to protect the security of the network, protect data integrity, and protect computer systems. These requirements were developed by the Information Technology Department. Changes to this document shall be communicated to all personnel. Please contact the IT service desk with any questions. ITServiceDesk@fortbendcountytx.gov or 281-341-4580.

Purpose

The requirements are designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a maximum time between changes to passwords.

Scope

The requirements apply to any and all personnel who have any form of computer account requiring a password on the organizational network including but not limited to a Computer login account and e-mail account.

Password Requirements

All personnel are responsible for adhering to these requirements set forth by the Information Technology Department, and failure to do so could result in revocation of computer access privileges. The most current guidelines shall be readily available on the County Intranet or by contacting the Information Technology Department Service Desk: ITServiceDesk@fortbendcountytx.gov, or 281-341-4580. A hard copy will be furnished on request.

- Minimum Length - 8 characters
- Passwords should contain at least 3 of the following:
    1. Upper case characters (A through Z)
    2. Lower case characters (a through z)
    3. Have at least 1 numeric character (0 through 9)
- Have at least 1 special character, the special characters are (!@#$%^&*_+=?/~`;:,<>|\)
- Combine short, unrelated words with numbers or special characters. For example: eAt42peN
- Make the password difficult to guess but easy to remember
- Substitute numbers or special characters for letters. (But do not just substitute) For example:
    - livefish - is a bad password
    - L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed
    - l!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable.

4. Characters that can be used - (!@#$%^&*_+=?/~`;:,<>|\).

Password Considerations
Passwords may not repeat more frequently than every 12 password changes

- Passwords will expire every 90 days
- Store passwords using reversible encryption - This should not be done without special authorization by the IT department since it would reduce the security of the user's password.
- Account lockout threshold - 5 failed login attempts
- Account lockout duration – 10 minutes after failed attempts.
- Workstation Screen savers will be set to require password entry after 15 minutes.
- Don't use common acronyms as part of your password.
- Don't use common words or reverse spelling of words in part of your password.
- Don't use names of people or places as part of your password.
- Don't use part of your login name in your password.
- Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
- Be careful about letting someone see you type your password.

Password Protection All personnel shall comply with the following:

- Never write passwords down. Never send a password through email.
- Never include a password in a non-encrypted stored document.
- Never tell anyone your password.
- Never reveal your password over the telephone.
- Never hint at the format of your password.
- Never reveal or hint at your password on a form on the internet.
- Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
- Never use your password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
- If you know or suspect that your password has been compromised, you should report it to the IT Department.
- If anyone asks for your password, refer them to IT Service Desk.

Other Considerations

System Administrator Passwords shall be changed within 24 hours or next business day upon termination of administrators. Administrator accounts should have the minimum access to perform their function. Administrator accounts are not to be shared.