INFORMATION TECHNOLOGY POLICY

Adopted October 14, 2014
Amended and Approved June 13, 2017

1 REVISION HISTORY

Revision	Author/Reviewer	Date	Changes
1.0	*Original Template Policy from Wood County* D. Parish T. Yarter	08/06/2014	
1.0.1	D. Parish, T. Yarter, S. Peal	10/09/2014	• Revise section 3 language to state IT Policy "supplements" the Personnel Policy • Revise section 9.2 to state Department Head determines when personal use is excessive
1.0.2	D. Parish, K. Byal, S. Peal		• Add section 6.1 Requests to Move/Relocate • Remove language in section 8.1 about moving hardware • Replace language in section 8.1 "brought to ITC for review" with "discuss with County Judge" • Add section 8.1.1 "Mobile Devices" to replace existing "iPad / Tablet Policy (2012)" • Remove redundant language from section 8.3 • Remove redundant statement from section 9 • Added Section 10 placeholder • Change section 11 "Weather Emergencies & Protection of Computer Equipment" to "Security" • Removed contradictory statement regarding sharing passwords and added additional password guideline to 11.1 • Add additional email safety precaution to section 11.3 • Revise section 11.4 regarding web filtering access approval procedures • Add section 12 "Mobile Devices" • Move existing "Weather Emergencies & Protection of Computer Equipment" to section 13

Approved this the 13th day of June, 2017 by the Commissioner's Court of Chambers County, Texas

Jimmy Sylvia – County Judge, Pro-tem
Gary Nelson

Jimmy Gore – Commissioner Precinct 1

Larry George – Commissioner Precinct 2

Gary Nelson – Commissioner Precinct 3

Rusty Senac – Commissioner Precinct 4

2 TABLE OF CONTENTS

3 INTRODUCTION STATEMENT

The policies and procedures set forth in this manual provide guidelines for management of employees during employment.

This document is used as a guideline to create base policies for users that will be connected to, accessing, storing data on, or transmitting data across the computer network owned and operated by Chambers County for the purposes of conducting its business.

The purpose of this document is to provide the County, its officials, its Department Heads, agents, contractors, and employees the basis for acceptable use of the County's technology resources. **This policy supplements the contents currently in effect found in the *Chambers County Personnel Policies Manual*. Should a conflict arise, the IT Policy supersedes the *Chambers County Personnel Policies Manual*.**

This policy has been reviewed and approved by the Commissioner's Court of Chambers County.

This policy requires that existing employees sign a written statement that they have read this policy and understand these guidelines prior to using any Chambers County computer equipment.

No usernames or passwords will be assigned until the new employee's signature has been obtained.

---

4 POLICY UPDATES

The Information Technology Department will update this policy as needed.
Once approved, IT will provide access to this policy on the County Intranet site.

---

5 POLICY VIOLATION

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

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

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

---

6 SUPPORT & INFORMATION TECHNOLOGY REQUESTS

Information Technology offers support for existing County computer systems by submission of an electronic Helpdesk ticket via the IT Helpdesk on the Employee Intranet.

Information Technology staff will attempt to resolve problems via remote control (when feasible). Non-operational *offices* will always take priority over non-operational *workstations* or other calls for service.

Using the Helpdesk for support ensures a timely response by the appropriate resource, documentation for tracking of problems, and data to pinpoint where resources might be concentrated in order to resolve ongoing problems.

6.1 Requests to Move/Relocate

No County Official, Department Head, or contractor shall move (or authorize to move) any County-owned computer equipment without first notifying the IT Department. The IT Department shall either move the equipment, or approve a user to move said equipment.
Offices that need to move standalone equipment and/or relocate employees with computer equipment must submit an IT Helpdesk ticket to have the move evaluated/completed.

Considerations for move and/or relocate requests:

- Must be submitted *at least* 2 days before the request needs to be filled
- During evaluation, if any cabling, power, and/or additional hardware is needed to complete the request, these prerequisites will need to be scheduled and installed prior to the request being completed
- Relocations needed or attempted without proper scheduling with the IT Department can lead to *preventable* downtime and will not be prioritized.

---

7 PURCHASING GUIDELINES

All purchases for technology related equipment and/or software must follow the policies and procedures set forth in the *Chambers County Purchasing Policy*.

All purchases for technology related equipment and software must first be approved by the Information Technology Department to ensure compatibility and/or compliance prior to purchase. This includes (but is not limited to) additional computers, phones, printers, printer leases, and/or any equipment that will need connection to the network, etc.

This approval request can be submitted via the IT Helpdesk by creating a service ticket with the description of the items/services in question. If approved, the request can be forwarded to the purchasing department.

In the circumstances where additional equipment is being added (new network printer/copier for example) the Technology Department must first be given time to do an assessment before an order is placed to verify that connections and all other requirements are available. If all requirements are not available, arrangements will need to be made to acquire anything needed prior to placing the order. Once this is completed the requesting department will need to confirm the installation date (even when done by a vendor) with the Technology Department. Failure to coordinate scheduling installation dates will result in rescheduling.

8 STANDARDS

IT has the responsibility for support and problem resolution for the County's computers and other computer related equipment. To effectively and efficiently carry out that role, IT must be able to rely on standard hardware and software configurations.

8.1 Hardware Standards

Department Heads who have a need to deviate from the standards must request an exception. The IT Director will review the request and approve the request as is, or suggest an alternate solution to ensure support can be provided by IT or the hardware provider. If a satisfactory solution cannot be agreed upon, the issue will be discussed with the County Judge.

Any County-owned technology equipment that is purchased without prior IT approval SHALL NOT be allowed to be connected to ANY County-owned computer, or to the computer network.

8.1.1 Mobile Devices

Apple iOS devices are the recommended standard for mobile devices without a full-featured operating system unless there is a technical or business need that requires an alternative solution that cannot be achieved with an Apple iOS device.

If the need to deviate from the recommended standard arises, the alternative solution will need to be discussed with the Information Technology Department prior to procurement.

Keeping a standardized fleet of devices allows for:

- Consistent user interface throughout the County's mobile devices
- Consistent management for policy implementation and patching for County mobile devices

8.2 Software Standards

IT must first acquire and test programs and executables before employees save them to their desktop computer. Software may only be used in compliance with the terms of the applicable license agreements.

8.3 Unauthorized Software

It is the responsibility of all Users in all departments to comply with maintaining the County standard by not downloading or installing unauthorized software onto any County owned PC, laptop, or other devices. Any software which needs to be downloaded and installed is to be done by IT. Unauthorized software is any software that is not approved for use by IT to conduct the business of Chambers County.

Examples of unauthorized use of software include streaming music, downloaded stock tickers, news reels, movie downloads, games, screensavers used from the Internet, unauthorized messaging software, etc.

Information Technology will:

1. Immediately inform the Department Head and if warranted, remove the unauthorized software in use when encountered.
2. On a routine basis, check and remove unauthorized software, unless the software has a legitimate business purpose for the User as determined by the IT Department and the appropriate Department Head.

---

9 TECHNOLOGY RESOURCE USAGE

Access to and use of the telephone network, computer network, Internet and/or email systems is provided to employees of Chambers County for the purpose of advancing the goals of the County.

All data, emails, email attachments, documents and other electronic information within the network/email system are the property of Chambers County.

THERE SHOULD BE NO EXPECTATION OF PRIVACY OR CONFIDENTIALITY IN COMPUTER NETWORK USE, INTERNET ACCESS, AND EMAIL USE ON THE COUNTY'S SYSTEMS.

Acceptable use always is lawful, ethical, reflects honesty, and shows restraint in the consumption of shared resources. Users shall refrain from monopolizing systems, overloading networks with excessive data or wasting computer time, connect time, disk space, printer paper, manuals or other resources.

9.1 Limited Personal Use

Authorized Users of the County may also use the Internet and email for limited personal use.

This is a privilege, not a right, and may be limited or removed at any time.

Users should also be mindful that the computers and other devices that are provided by the County are the property of Chambers County and must be treated as such, and are not to be used by users as personal home computers or computers to store personal documents, photographs, music, etc. Chambers County does not accept liability for any loss or damage suffered by an employee as a result of that employee using the County Internet connection for personal use.

Occasional, limited, appropriate, personal use of the computer system is permitted when the use does not:

1. Interfere with the User's work performance.
2. Interfere with the normal operation of your department or work unit.
3. Interfere with any other User's work performance or have a negative impact on overall employee productivity.
4. Have undue impact on the operation of the computer system.
5. Cause any additional expense or load to the County or department.
6. Compromise your department or the County in any way.
7. Violate any other provision of this policy, any other policy guideline, any law/regulation, or standard of Chambers County.

9.2 Inappropriate Use

The use of public resources for personal gain and/or excessive private use by any User are absolutely prohibited and punishable by applicable County disciplinary procedures, which may include termination and/or criminal prosecution depending upon the nature and severity of the transgression. Use is determined to be "excessive" by the Department Head or Elected Official.

9.3 Computer Data Backup

User data and documents are a County asset and should be treated as such. For this reason, files on managed network drives are backed up daily.

The responsibility of backing up files or individual computers is that of the Users. Storage only on a PC hard drive is a risk in that if the hard drive fails, the data may not be recovered. While files stored on network shares are backed up automatically each night, Users must be proactive in making sure that their files are backed up for safekeeping. This can be done in coordination with the IT Department.

Please note that if a User's computer hard drive becomes damaged, there is no guarantee that the information on it will be recoverable.

---

10 <PLACEHOLDER FOR FUTURE SECTION>

---

11 SECURITY

Prior approval from IT must be obtained before any of the following activities are attempted. These are not allowed by default:

- Connecting any networking devices to the County network.
- Usage of modems on individual servers / desktops / workstations for remote access purposes.

- Allowing non-County agencies or entities to access the County network without prior IT approval.
- Allowing ANY person who is not employed by Chambers County access to any computer or private network connection.

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

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

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

11.1 User Accounts & Passwords

Users are responsible for safeguarding their passwords for access to the computer system. Users are responsible for all transactions made using their passwords.

Users are expected to follow these guidelines when possible:

- Passwords shall remain confidential and should not be printed or given to others.
- Passwords shall be changed every 90 days (automatically in required systems).
- Passwords shall be at least eight characters long.
- Passwords shall contain characters from at least three of the following four classes:
    - English upper case letters, A, B,
    - English lower case letters, a, b,
    - Westernized Arabic numerals, 0,1,2, and
    - Non-alphanumeric ("special characters") such as punctuation symbols.
- Passwords shall not be a dictionary word or proper name.
- Passwords may not contain your User name or any part of your full name.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- The password shall not be a computer term, name, command or a site, company, hardware, or software name.
- The password shall not be your birthday or other personal information such as address and phone number.
- The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc.
- The password shall not be any of the above spelled backwards.

11.2 Local Computer Security

Please follow the guidelines below to help avoid security breaches:

- Close sensitive or confidential applications **and lock your computer when you leave your desk**.
- Do not leave portable media such as CDs or floppy disks in drives.

- Turn off your computer when you leave for extended periods.
- Never write your passwords on a sticky note or try to hide them anywhere in your office.
- Where appropriate:
    - Use a screen filter to minimize the viewing angle on a computer monitor.
    - Enable a password-protected screen saver.

11.3 Antivirus Protection

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

In some cases, simply reading an email can spread a virus to a User's computer, and from there to many other internal and external County recipients. The County will take prudent measures to scan incoming email and attempt to intercept viruses; however, no safeguard is foolproof.

Each User is responsible for taking reasonable precautions to avoid introducing viruses into the County network, including but not limited to:

- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- NEVER open any email attachments from county employees or trustworthy senders unless you were expecting the email or contacted the sender to verify it was something that was intended to be sent.
- Delete and never forward spam, chain, and other junk email.
- Never download files from unknown or suspicious sources.
- Always scan external drives (floppy, flash, DVD, etc.) from external or unknown sources for viruses before using it.
- Back up critical data and system configurations on a regular basis and store the data in a safe place.

11.4 Firewall & Web-Filtering

The County uses a firewall and web-filtering system to help the County network stay secure and ensure that internet resources are not being misused.

Black-listing: There are some sites that will be blocked by the IT Department whenever use of those sites is felt to have a negative influence on employee performance by a Department Head. Department Heads can request that additional sites become black-listed (blocked) to the IT Department via the IT Helpdesk on the Chambers County Intranet who shall make every effort to investigate the feasibility of such a block.

White-listing: Department Heads may also request that blocked sites become white-listed (allowed) if the sites are needed for their job duties. *The request to white-list a site should be submitted via the IT Helpdesk on the Intranet with detailed information as to why the white-listing of the site is being requested.*

The IT Network Security department will discuss requests for additional access with the County Judge. Recommendations will be made against requests that pose a security risk and/or do not promote the goals of Chambers County; however, the final decision to approve or deny the request will be that of the County Judge.

11.5 Network Monitoring

All computer applications, programs, data and work-related information created or stored by County employees on County information systems and resources are the property of Chambers County.

The County IT Department reserves the right to access and monitor computer related transmissions, as well as stored information, created or received by County Users with County Information Technology systems and resources under the following circumstances:

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

11.6 Interdepartmental Access

Each department within the Chambers County Computer network is separated by means and measures to prevent unauthorized access.

No department (with the exclusion of the Information Technology Office) may access any other department in the Chambers County Computer network without written consent of the involved Department Heads.

Any official, Department Head, employee, etc. that attempts to circumvent the security measures in place to gain unauthorized access to any data, computer, or other network subnet may be subject to severe criminal penalties and possible civil liabilities.

11.7 Access Removal

The Department Head (or authorized designee) must submit a service request upon employee departure or termination. The request should reflect all systems for which a terminated employee had access.

Please note if email or file data is to be transferred to the Department Head's account or other location, otherwise, any-and-all data associated with the account will be deleted.

Persons no longer employed have no right to the contents of their email messages or data stored in County systems, and should not be allowed access to the internal system.

11.8 Physical Intrusion & Panic Alarm Systems

Chambers County employs several types of protection alarm systems in the main courthouse building and annexes, along with the Tax Office and remote Sub-Courthouses. Although the IT Department is not responsible for the security of the buildings, the IT Department does coordinate with the vendors where applicable for network/software configurations.

---

12 MOBILE DEVICES

Mobile devices (such as smartphones and tablet computers) represent a significant risk to information security. This section of the policy intends to protect Chambers County data from a breach which could result in loss of information, damage to applications, and also damage to the County's public image.

12.1 Mobile Device Management

Mobile Device Management provides the tools to centrally manage, control, and monitor mobile devices.

All County-owned mobile devices shall be managed by the IT Department's Mobile Device Management system if any of the following conditions apply:

- The mobile device requires setup assistance
- The mobile device requires technical support
- The mobile device will be used to access any County data systems
- The mobile device will connect to any County networks

12.2 County Mobile Device Requirements

- Device must still be supported by the manufacturer and receive regular updates
- Device must be configured for local device authentication
- Device must not be jailbroken or rooted
- Remote locking and wiping will be enabled
- Mandatory policy settings will be applied
- Location services will be enabled for device tracking
- Device will be automatically wiped after 10 failed access attempts

12.3 Access from Personal Mobile Devices

Simple convenience may not serve as criteria for enabling access to County data systems (including email) on a personal mobile device. Additionally, supervisors must ensure that the requirements for non-exempt employees to access County data systems after normal working hours are clearly understood and explained.

Said requirements should also be in compliance with the Fair Labor Standards Act and the overtime / compensatory time regulations in the Chambers County Personnel Policy.

The Information Technology Department is not responsible for ensuring connectivity to or compatibility with County data systems (including email) from personal mobile devices.

With the exception of confidential information, there can be no expectation of privacy related to County business conducted using a personal mobile device. Personal mobile devices that access County data systems may be subject to public information requests or legal investigations if pertinent data exists on the device.

Any data overage charges incurred as a result of conducting County business from a personal mobile device are not the responsibility of the County.

Chambers County will not be responsible for the loss of data on a user's personal mobile device. Users should make sure to keep a current backup of their mobile device data.

12.3.1 Personal Mobile Device Requirements

Access to County data systems will be terminated for any personal mobile device failing to conform to the following requirements.

- Information Technology will enforce security regulations that require an unlocking mechanism to be used to access the device (PIN, password, etc.)
- The owner of a personal mobile device must report a lost or stolen device immediately to Information Technology so the device can be remotely wiped
- The owner of a personal mobile device must report an upgrade / replacement prior to changing devices so that County data can be properly removed. If Information Technology was not allowed to remove the County data prior to the upgrade / replacement the device may need to be remotely wiped.
- Device must not be jailbroken or rooted or the device may be remotely wiped.

Note: The discussion of a remote wipe will initiate if a device is rooted/jailbroken (hacked), lost, stolen, or upgraded / replaced without notification to Information Technology. Information Technology will obtain written consent from the County Judge before performing a remote wipe.

12.3.2 Personal Mobile Device Access Requisition

- A business need must be expressed in order to gain access to County data systems from a personal mobile device
- The request for access to County data systems from a personal mobile device must be submitted by the Department Head / Elected Official via email or IT Helpdesk Ticket
- Requests not submitted by a Department Head / Elected Official will not be accepted
- Changes in position / department may require re-approval

13 WEATHER EMERGENCIES & PROTECTION OF COMPUTER EQUIPMENT

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

- Backup current copy of important files.
- All computer equipment should be powered off. After powering down the equipment, disconnect the power cables from the receptacles to protect equipment from potential electrical surges.
- Any equipment located on the floor should be moved to a higher location and away from any windows.
- Cover all equipment with plastic sheeting/bags and secure with masking tape. The purchasing of plastic bags and/or masking tape is the responsibility of the individual departments.