

**MONTGOMERY COUNTY, TEXAS
EMPLOYEE POLICY MANUAL
3. EMPLOYEE RESPONSIBILITIES**

3.4 TECHNOLOGY POLICY

**COMPUTER/PC USE
AND SCOPE**

3.4-1 This policy applies to all internet access, electronic communications, software and computer equipment attached to or used on the Montgomery County network system (including equipment owned by outside agencies and individuals) and applies to all Montgomery County owned software and hardware regardless of location or connectivity; it applies to all individuals using the Montgomery County network system whether or not they are employees of Montgomery County. The intent of this policy is to permit maximum freedom of use consistent with federal and state law, Montgomery County policy, and a productive working environment.

3.4-2 Use of Montgomery County computers and communication devices must comply with Texas law and Montgomery County policies. Therefore, Montgomery County computers and communication devices may not be used for commercial, profit-making or political purposes, or to disseminate unsolicited information regarding religious or political beliefs. With the rapidly changing nature of electronic media developing among users of external on-line services and the Internet, 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 Internet service and e-mail by all County departments.

3.4-3 Employees are responsible for complying with this policy. In order to ensure that employees are aware of the provisions of this policy, they will be required to acknowledge acceptance of same before being allowed access to Montgomery County's electronic communications equipment other than telephonic. Elected officials and department heads are responsible for taking disciplinary action against employees in violation of this policy.

**COMPUTER
SECURITY**

3.4-4 Each department and each user must maintain a high level of physical security for each machine entrusted to the care of that department and that individual to prevent unauthorized access to the Montgomery County network. When an employee has logged onto the network, the level of access to the network available to that employee is available to anyone using that computer. Thus, anyone sitting at the computer (visitors, reporters, contractors, janitors, jail inmates or trustees) will be able to view, change, and enter the same data that the employee logged onto the system is allowed to view, change or enter. Not only does this compromise the integrity of the data on the Montgomery County network, in some cases it is illegal to disclose the information on the network without a court order or permission from a specific person. Therefore, all employees should take the following steps:

3.4-5 At the end of the day or shift, logout and turn off power to your equipment. If the equipment is being used for remote access, you must logout, turn off power to the equipment, and then turn power back on to the equipment (but not log in), before leaving for the day.

**MONTGOMERY COUNTY, TEXAS
EMPLOYEE POLICY MANUAL
3. EMPLOYEE RESPONSIBILITIES**

3.4 TECHNOLOGY POLICY

3.4-6 Allowing others to use your password is a serious breach of security. Do not divulge your password to anyone. If *any* person requests your password for any reason whatsoever, please report this immediately to your elected official or department head. He/she should report this to Montgomery County Communication Information Services (CIS). CIS should never have the need to know your password; should the occasion ever arise, secured procedures will be established by the CIS Director. Do not select a password that anyone who knows you could easily discern. Select one with a combination of letters and numbers that you can remember.

3.4-7 The sharing of computer data by using Windows file-sharing techniques is prohibited. Other more secure techniques, such as e-mail attachments, can be used to accomplish the same task.

3.4-8 Non-employees are expressly forbidden from using any terminal (except the public access terminals) without proper authorization. Should an elected official or department head have a need for a non-employee to access data other than through the public access terminals, he/she may request authorization through CIS.

3.4-9 If you must write down a password or user-ID, always maintain physical control over the document (keep it in wallet or purse). Do not:

- A. Identify the password as being a password.
- B. Record it in a document or file.
- C. Include the login name on the same piece of paper.
- D. Attach the password to a pc/terminal, keyboard, or desk.
- E. Write it down exactly as it is entered.
- F. Give the password to anyone over the telephone (including tech support).
- G. Send the password to anyone by e-mail.

3.4-10 If you have remote access to your computer from home or an outside agency has access, the dial in communication software must never be configured in such a way as to make the connection providing the password in the process. The attachment process **must require the manual entry** of the password. We have no way to control the individuals who may have physical access to a users' computer, whether at home or in a service center or otherwise.

3.4-11 Computers attached to the Montgomery County network authorized to be controlled remotely from home or another location must be configured to be waiting for a connection, but not logged into the network. In this way all security that is in place at work is also in place remotely, in addition to the dial-in security. Any computer attached to the Montgomery County network used for remote access must be configured to dial-back the remote computer.

**MONTGOMERY COUNTY, TEXAS
EMPLOYEE POLICY MANUAL
3. EMPLOYEE RESPONSIBILITIES**

3.4 TECHNOLOGY POLICY

PROHIBITIONS

3.4-12 Do not:

- A. Attempt to read or “hack” into other systems or other persons’ log-ins, or “crack” passwords, or breach computer or network security measures.
- B. Seek others’ passwords or exchange passwords.
- C. Develop programs designed to harass other users or infiltrate a computer or computer network or to damage or alter hardware or software.
- D. Use your computer or network services in a manner that is likely to cause network congestion or significantly hamper the ability of others to access and use the services or equipment.
- E. Intentionally seek access to or copy information, files, or data which is confidential under federal, state, or local law unless specifically authorized to do so once the legal conditions for release are satisfied.
- F. Attach private equipment and/or use private services for the express purpose of circumventing this policy.
- G. Participate in the development, propagation or forwarding of computer viruses.
- H. Allow or provide access for unauthorized personnel to use the County’s network system including internet service and e-mail.

APPLICABLE LAWS

3.4-13 Federal Copyright Law: Many intellectual works are copyrighted. The owner of a copyright holds the exclusive right to reproduce and distribute the work. Most computer programs and manuals are copyrighted, and care must be taken to comply with copyright laws.

3.4-14 State and Federal Trade Secret Laws: Many intellectual works are protected under trade secret laws. Owners consider some programs and many manuals trade secrets, and there are civil and criminal penalties associated with disclosing this information to anyone not authorized to use the material. Unless authorized in writing by the owner of the trade secret, you should not disclose any material that contains trade secret declarations to anyone outside County government.

3.4-15 Software License Agreements: Most computer software is licensed to a specific user or a group of specific users, and the license agreement is very specific as to the rights that the user has to operate the program and make additional copies of the program. There are civil and criminal penalties associated with breaking a license agreement.

**COMPUTER
SOFTWARE**

3.4-16 Montgomery County provides computers to its employees with software pre-installed. The County encourages employees to use this technology to enhance their efficiency and effectiveness in providing services to the citizens of Montgomery County. Since the County uses a fully integrated network system, any change to a single computer can affect the rest of the Montgomery County network; because of this and due to our limited resources, the following procedures are mandatory.

**MONTGOMERY COUNTY, TEXAS
EMPLOYEE POLICY MANUAL
3. EMPLOYEE RESPONSIBILITIES**

3.4 TECHNOLOGY POLICY

A. Unless provided by a state or federal agency, Montgomery County must own a software license for all software used on County-owned equipment unless prior authorization has been obtained from CIS.

B. Outside agencies with equipment attached to the Montgomery County network must provide proof of licensing for any software used with that equipment. Excepted is state or federally required software where the particular state or federal agency holds the license.

C. All software on any computer attached to the Montgomery County network or any other computer owned by Montgomery County must be installed/uninstalled, configured and/or updated by CIS or individual departmental representatives approved by CIS. This includes games, desktop themes, screen savers, etc., utilities not originally installed.

D. All Montgomery County computer software shall be approved by CIS and ordered by the Purchasing Department. Outside agencies must have CIS approval for software that is to be used on equipment attached to the Montgomery County network before it is obtained. Excepted is state or federally provided hardware and software.

E. Purchase of software specific to a department, specialty software, or software to meet personal preferences must be funded by the department but approved by CIS and ordered by the Purchasing Department. Excepted is state or federally provided software. Training for such specialty software shall be the responsibility of each department.

F. Departments will fund purchases of additional computer software licenses due to departmental growth. Net Term and Unidata software licenses will be provided by CIS.

**INTERNET SERVICE/
E-MAIL**

3.4-17 Internet service and e-mail are provided to selected Montgomery County employees (based on need), contractors, vendors and other persons or firms designated by authorized County officials for conducting Montgomery County business. Every elected official, department head, and employee has the responsibility of maintaining and enhancing the County's public image and to use County e-mail and the Internet in a productive manner.

3.4-18 Montgomery County realizes that e-mail can be an efficient means of communication, similar to the telephone. Therefore, the County will allow for the use of e-mail for personal communications. However, this practice should be limited and should not interfere with your work responsibilities. To ensure that all employees are responsible, the following e-mail and Internet policy are established. Any improper use of the Internet or e-mail is not acceptable and will not be permitted.

**MONTGOMERY COUNTY, TEXAS
EMPLOYEE POLICY MANUAL
3. EMPLOYEE RESPONSIBILITIES**

3.4 TECHNOLOGY POLICY

3.4-19 Employees on the County's Internet service and e-mail may not transmit copyrighted materials. All users obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission, or as a single copy for reference purposes only.

3.4-20 Users of the County Internet service and e-mail should conduct themselves in a professional manner. Access to the County Internet service and e-mail is a privilege, not a right, which may be revoked for inappropriate conduct. It is the responsibility of every user to report any known misuse of the Internet or e-mail to his immediate supervisor.

**EMAIL OPERATIONS
& BACKUP**

3.4-20a Read, unread, and sent mailbox messages will be retained automatically by the e-mail system for not more than 30 days. Deleted items will be deleted automatically one (1) day after deletion from the mailbox. Manually deleted "Deleted Items" are not retained in any way. Routine backups are made of the e-mail system and are maintained for seven (7) days. However, backups of the e-mail system are created and maintained for the recovery of the system only. Backups are not intended as permanent record retention storage.

OWNERSHIP

3.4-21 All messages or files created, sent, retrieved or downloaded over the County's e-mail/Internet system are the property of the County. With the exception of information made confidential by State statute, the County reserves the right to access and monitor all messages and files on the County's e-mail/Internet system. Do not assume electronic communications are private and do not transmit highly confidential data using this medium without appropriate protection. All electronic and telephonic communications systems and all information transmitted by, received from, or stored in these systems are the property of Montgomery County. County employees and other users of the County's electronic and telephonic communications systems have no expectation of privacy or any personal privacy right in connection with the use of these systems, or with the transmission, receipt, or storage of information in these systems.

MONITORING

3.4-22 Elected officials and department heads have the authority to request CIS to inspect the contents of any equipment, files, calendars, or electronic mail of their subordinates in the normal course of their managerial responsibilities. Reasons for review include, but are not limited to, system hardware or software problems, general system failure, regular system maintenance, a lawsuit against Montgomery County, suspicion of a crime or violation of policy, review of employee work, a need to perform work, or to provide a service.

**MONTGOMERY COUNTY, TEXAS
EMPLOYEE POLICY MANUAL
3. EMPLOYEE RESPONSIBILITIES**

3.4 TECHNOLOGY POLICY

**RETENTION OF
ELECTRONIC
RECORDS**

3.4-22a All e-mail documents and accounts are subject to Public Records Law unless otherwise exempt. Users shall comply with public retention laws and rules.

**RELEASE OF
ELECTRONIC
RECORDS**

3.4-23 Release of electronic records pursuant to a request for public information is governed by Chapter 552, Texas Government Code. A request for public information must be in writing. Should you have a question about a particular request received in your department, contact the County Attorney's Office as soon as possible.

3.4-24 All communications sent electronically by employees via Montgomery County's Internet service and e-mail must comply with this and other County policies and may not disclose any confidential or proprietary County information.

**ACCEPTABLE
USES OF INTERNET
AND E-MAIL**

3.4-25 The following is a non-exhaustive list of acceptable uses of the internet and e-mail:

- A. Communication and information exchange directly related to the duties or responsibilities of the user's department.
- B. Communication for professional development, to obtain continuing education or training, or to discuss issues related to the user's public duties or responsibilities.
- C. Announcement of new departmental regulations, procedures, policies, rules, services, programs, or activities.
- D. At the elected official/department head's discretion, employees are permitted to use the Internet service and e-mail for incidental personal matters.

3.4-26 The following is a non-exhaustive list of unacceptable uses of the internet and e-mail:

- A. Software Downloads:
 - 1. No software or internet utilities may be downloaded or installed on systems described above without the express approval of CIS. Such software and utilities can and have changed fundamental system configurations rendering the equipment inoperable for other County users.
 - 2. Unless specifically authorized by the elected official/department head and CIS, downloading or streaming of MP# and other music files, video files, TV or radio programs, browser enhancements such as plug-ins that must be downloaded to view a document, is prohibited.

**MONTGOMERY COUNTY, TEXAS
EMPLOYEE POLICY MANUAL
3. EMPLOYEE RESPONSIBILITIES**

3.4 TECHNOLOGY POLICY

- B. County internet service and e-mail must not be used for knowingly transmitting, retrieving, or storing any communications that contain:
1. Discriminatory or harassing language.
 2. Obscene, pornographic or x-rated material.
 3. Defamatory, abusive, threatening, profane or offensive language.
 4. "Chain" letters and other non-business-oriented mass e-mails.
 5. Derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference.
 6. Racial and/or sexual slurs or jokes.
 7. Any material which is illegal or against County policy.
- C. Identity Masking: No e-mail or other electronic communication may be sent which:
1. Attempts to hide the identity of the sender or represents the sender as someone else.
 2. Adopts the identity of another person.
 3. Uses another person's password.
 4. Misrepresents the user's affiliation with Montgomery County.
- D. Business Use: Except as specifically authorized above, all use of Montgomery County's Internet service and e-mail must be for the benefit of Montgomery County and must not be used:
1. For any personal profit.
 2. For purposes not directly or indirectly related to the job duties or responsibilities of the user before, after, or during normal business hours.
 3. For any non-County commercial or promotional purpose, including personal messages offering to buy or sell goods or services.
 4. To sell or distribute Montgomery county information, software, or services for personal gain or profit.
 5. In such a way that causes Montgomery County to be charged a fee by another person or entity.
- E. Restricted Information: Montgomery County's Internet service and e-mail must not be used:
1. To copy, retrieve, or forward copyrighted material (such as software, databases, documents, articles, graphics, and downloaded data) unless the individual has the right to copy or distribute such material.
 2. To communicate any material regarding confidential information from a person's personnel file, medical record, or information regarding a person's health condition, financial status, or a person's home address, telephone number, or social security number, unless expressly authorized to do so utilizing appropriate protection.

**MONTGOMERY COUNTY, TEXAS
EMPLOYEE POLICY MANUAL
3. EMPLOYEE RESPONSIBILITIES**

3.4 TECHNOLOGY POLICY

F. Internet Access Through “Dial-up” Instead of Network Access: Use of personal Internet service providers (such as AOL) using telephone dial-up or other telephone access to the Internet is prohibited. Written requests for a waiver must be submitted to CIS.

WEB SITE

3.4-27 The Montgomery County web site and associated home pages have been established at the direction of Montgomery County Commissioners Court to improve the quality, productivity, and general cost effectiveness of the County’s workforce, as well as greatly enhance communications between the public and Montgomery County. The quality of the layout, timeliness of information contained in the site, categories of information on the home pages, and subsequent web pages will be at the elected official/department head’s discretion. The Montgomery County home page will link County departments and other web pages and sites to provide readily available information to all users. All proposed home pages and associated web pages will be professional in appearance and will contain current and accurate information, while emphasizing information that is important to the citizens of Montgomery County.

3.4-28 The elected official/department head and CIS are the approving authorities for all official Montgomery County web pages including design, layout, and content.

3.4-29 Access to official County data (databases, images, documents, etc.) must be through the responsible Montgomery County elected official or department head who maintains the data and CIS.

**VIOLATION OF
POLICY**

3.4-30 Violation of this policy can lead to internal disciplinary action, up to and including termination of employment. In addition, criminal or civil administrative penalties may be imposed. Security violations will be reported to your elected official or department head and may result in your password and access to the network being revoked.

3.4-31 In the event that Montgomery County incurs a cost due to employee negligence or misuse, the employee will be responsible for reimbursement of that cost.

3.4-32 There are a number of state and federal laws regarding computer crimes. Certain violations may result in a person being charged with a criminal offense, ranging from a Class A misdemeanor to a first-degree felony.