Howard County, Texas Technology Usage Policy

2 Table of Contents

3 Introduction

The policies and procedures set forth in this manual provide guidelines for management of employees during employment, but do not create contractual rights regarding termination or otherwise. This policy supersedes any policies already in effect in county departments as enacted by the official or department head over the respective department. This document is used as a guideline to create base policies for users that will be connected to, accessing, storing data on, or transmitting any other data across the computer network owned and operated by Howard County for the purposes of conducting IT business. The purpose of this document is to provide the county, IT officials, IT department heads, agents, contractors, and employees the basis for acceptable use of the county's technology resources.

This policy has been reviewed and approved by the commissioners court of Howard County. All authority granted to the parties named within was vested in the open meeting of the Howard County Commissioner's Court on: _____

In order to maximize the benefIT of the Information Technology investments across Howard County, the Information Technology Services (IT) department has created this Technology Usage Policy as a way to address and communicate existing and new policies. Goals of this policy are:

1. Support the overall Vision and Goals of Information Technology Services.
2. Protect confidential, proprietary information of the county from theft or unauthorized disclosure to third parties;
3. Be cost-effective and prevent waste of information technology (IT) resources;
4. Reduce, and if possible, eliminate, potential legal liability to employees and third parties

This policy requires that all new and existing employees sign a written statement that they have read this policy and understand these guidelines.

3.1 Information Technology Services Vision Statement

Provide value-added technical services and solutions to Howard County that enhance or enable better service to our citizens and employees.

3.2 Goals

- Ensure the availability and security of our network
- Enable ease of obtaining and sharing of data.
- Lower costs - Achieve IT Standardization where feasible
- Better enable disaster recovery of critical systems.

3.3 Guiding Principles:

- IT will provide quality customer service and solutions.
- IT will demonstrate professionalism and be customer focused – to our citizens, County teammates, and business partners.
- IT will maximize our information technology investment by fully leveraging our solutions and services possible across the County.
- IT will promote and implement standard technology and solutions, where feasible, throughout all County offices to support common business processes.
- IT will use commercially available software packages wherever possible.
- IT will dynamically re-engineer our business processes around the functionality of available application packages.
- IT will work efficiently using best practices.

4 Communication

IT will update this policy, as needed, and once approved, will communicate the updates to all Department Heads and IT Contacts, as appropriate. IT will also provide access to this policy on the County website. The County will use reasonable efforts to notify Users when software patches or other software is deployed to User PCs and where there may be a disruption to the User. There will be times where software will need to be deployed where prior notice may not be feasible, as in the case where there is a **security risk or legal/statutory compliance requirement** or where such deployment is transparent to the user, as in the case of operating system or application upgrades; asset inventory data collection, data collection for license management and compliance, or for new software that the county deploys and which can occur in the background without disruption to the User.

5 Standards

IT has the responsibility for support and problem resolution for the County's PCs and network. To effectively and efficiently carry out that role, IT must be able to rely on standard hardware and software configurations on the desktop. Users must request hardware and software through Information Technology.

5.1 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 either approve request as is or suggest alternate solution to ensure support can be provided. If a satisfactory solution cannot be agreed upon, the issue will be raised to the appropriate member of the Howard County Commissioner's Court.

The IT Department is responsible for the configuration and acquisition of ***ALL*** county-owned technology equipment that will interface with the county computer network at any level or connected to any computer or device that is connected to the county computer network, regardless of what fund pays for said equipment. **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.** The IT Department shall have uninhibited access to all county-owned computer equipment that is connected to the county computer network for inspection and inventory control upon request at any time.

Due to security configurations of the county network, no County official, department head, employee, or contractor shall move or authorize to be moved any county-owned computer equipment that is connected to the county computer network without first notifying the IT Department. The IT Department shall either move the equipment or approve a user to move said equipment. If a user moves any equipment, and does not inform the IT Department, the device will not function at IT new location due to network configurations.

5.2 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.

The Software Standards specify the technologies supported by the organization and serves as a guideline for all technology purchasing and use decisions, including hardware, software, peripherals, and network components. Current software standards are listed on the County's intranet site.

5.3 Unauthorized Software

Use of unauthorized software can degrade the county's network and Internet service, create security risks and personal computer problems, divert focus from county-related issues, reduce employee productivity and increase costs. 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 or laptop. 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 Howard County.**

Information Technology Services will 1) immediately inform the department head and if warranted, remove the unauthorized software in use when encountered and 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

6 Network Resource Usage – Internet, Email & Data

Access to and use of the Computer network, Internet and/or e-mail systems is provided to employees of Howard County for the purpose of advancing the goals of the County. This access imposes certain responsibilities and obligations on County employees, (full-time, part-time and temporary employees), officials, and as well as any companies or individuals (third parties) contracted to do work for the County, or use County IT resources, (hereinafter termed "Users") and is subject to County government policies and local, state and federal laws. All data, e-mails, e-mail attachments, documents and other electronic information within the network/e-mail system are the property of Howard County. **THERE SHOULD BE NO EXPECTATION OF PRIVACY OR CONFIDENTIALITY IN COMPUTER NETWORK USE, INTERNET ACCESS AND E-MAIL USE ON THE COUNTY'S SYSTEMS.** The County, acting through IT managers and supervisors, has the capability to view data and e-mail at any time. Whereas all county employees are allowed access to the Internet, only full time employees are allowed E-Mail accounts within the County's system. Part-time and temporary employees are not granted e-mail address by default. If a need exists for said employees to have access to the county e-mail system the department head should express that to the IT Director who will determine if there is enough free e-mail boxes to make the allocation and inform the Department Head making the request. The IT Director shall have the final decision in the allocation of e-mail resources. This policy does not supersede any state or federal laws regarding confidentiality and appropriate use.

The primary purpose for using the County's Computer or Telephone network, Internet and e-mail connection is in advancing the business of the County. This includes, but is not limited to:

- Communication with, and providing service to, clients and citizens of Howard County.
- Conducting the business of your department or unit
- Communicating with other employees for work-related purposes.
- Gathering information relevant to your duties or to expand your expertise.

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. County users may be subject to limitations on their use of the networks, or other action, as determined by the appropriate supervising authority. Users are also expected to cooperate with any investigation regarding the use of your computer or your activities associated with Information Technology resources.

Content of all electronic communications should be accurate. Users should use the same care in drafting email and other electronic documents as they would for any other written communication.

As with internal e-mail messages, Internet e-mail can be changed by outside parties and forwarded to others without the employee's knowledge or permission. Users must use caution in using Internet e-mail and must

comply with all state and federal laws. Access or interception of other's e-mail is a violation of state and federal law and will be reported to the appropriate authority for investigation and possible prosecution.

User data and documents are a County asset and should be treated as such. For this reason, Users who have access to a shared network drive should store all data files on the shared drive as these files are backed up daily. Recovery of data stored on desktops is the User's responsibility. Storage only on a PC hard drive is a risk in that if the hard drive fails, the data may not be recovered.

6.1 Limited Personal Use

Authorized Users of the County may also use the Internet and e-mail for **limited personal use**. This is defined as any personally initiated online activity (including e-mail and Internet usage) that is conducted for purposes other than those listed above. ***This is a privilege***, not a right, and may be limited or removed at any time by management. Howard 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 (It shall be infrequent and brief.).
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, i.e., HIPAA, or standard of Howard County.

6.2 Inappropriate Use

The use of public resources for personal gain and/or excessive private use, such as but not limited to the items listed below, by any User is 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. The term public resource as used in this policy includes not only the unauthorized use of equipment, hardware, software or tangible articles, but also the employee time expended in the engagement of the unauthorized use while on County time.

Examples of unauthorized use of software include streaming music, stock tickers, news reels, etc., to the desktop, movie downloads, games, screensavers used from the Internet, unauthorized messaging software such as AOL, YAHOO, Windows Messenger; and "chat" software.

Employees may not:

1. Use IT resources for personal gain, or to support or advocate for non-County related business or political purposes.
2. Create, distribute, upload or download any disruptive, abusive, harassing, threatening, or offensive messages, including offensive comments or graphics about sex, race, gender, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
3. Use IT resources for illegal or unlawful purposes or to support or assist such purposes.
4. Use IT resources for wagering, betting, or selling chances or to support or assist such purposes.
5. Use IT resources for personal long distance telephone calls.
6. Attempt to circumvent or subvert system or network security measures, provide internal network access to any non-Users or use your account to gain unauthorized access to external networks and systems.

7. Mount an attack on the security of any system (i.e. attempting to hack or introduce viruses into a system).
8. Use the network to disrupt network Users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer "worms" and viruses, and sustained high volume network traffic that substantially hinders others in their use of the network.
9. Intercept network traffic for any purpose unless engaged in authorized network administrative duties.
10. Install or use encryption software on any Howard County computers without first obtaining written permission from your Department Head and IT. Users may not use encryption keys or encryption passwords that are unknown to their Department Head.
11. Engage in online fundraising (unless approved by Department Head or Official)
12. Engage in mass-mailing or send County-wide messages without department head approval.
13. Send County-wide mailings about viruses, or other warnings about outside computer attacks (these are almost always a hoax and should be turned over to IT for disposition).
14. Initiate or forward chain letters by email.
15. Spoof (disguise) your identity or send anonymous e-mails or send e-mail under another employee's name without permission.
16. **Download any non-standard or non-business-related files or software, including "freeware" and/or "shareware" programs unless previously approved.**
17. Load personal Internet Service Provider accounts (i.e. AOL, CompuServe, etc.) on County owned equipment.
18. Unless expressly authorized, sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of the county is strictly prohibited. Unauthorized disseminating of this information may result in substantial civil liability as well as severe criminal penalties under the Economic Espionage Act of 1996. Employees must obtain permission from their Department Head to gain access to the County's Internet facility.
19. Make or use illegal copies of copyrighted software or other mediums, store such copies on County systems, or transmit them over the County network.
20. "Rip" music CDs and store said music in the My Documents folders or any other folders that are located on county owned servers. This is a waste of county resources and server storage space and can potentially have a negative effect on county business.

It is the shared responsibility of all county employees, the supervisor, manager and/or department head, and the IT Department to be aware of how the County's Internet facility is being utilized by his/her employees and ensure that employees are periodically informed and aware of the IT policies at a minimum on an annual basis.

6.3 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 Howard County. Howard County employees shall have no expectation of privacy in anything they store, send, or receive on the County's computer systems. Data may be monitored without prior notice. The County IT Department reserves the right to access and monitor e-mail use and any other 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 during 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

The reservation of this right is to ensure that public resources are not being wasted and to ensure the County's information systems are operating as efficiently as possible in order to protect the public's interests. This includes blocking access to certain Web sites for which access is deemed to be in conflict with County policy.

6.4 E-Mail Records Retention

Users are cautioned that deleting an e-mail message from a User's own mailbox does not mean all copies of the message are also deleted. The message may still reside in the recipient's mailbox, may have been saved in some other folder, or forwarded to other recipients. Also, any message sent the day before may be saved in the nightly system backup and retained for 5 years.

IT will NOT be held liable for any e-mail that is deleted that should have been retained pursuant to records management requirements it is the responsibility of the user to ensure they comply with records management requirements.

As with other records, no e-mail record may be destroyed after it is requested for reasons including but not limited to: employee termination & disciplinary action, until: a) the request is granted, or b) 60 days have elapsed after the request is denied or c) litigation on the records availability is complete and any court order has been obeyed.

Managers and supervisors may, with Department Head approval, access, as necessary, an employee's e-mail if employees are on leave of absence, extended leave, or are transferred from one department to another.

6.5 Data Storage

IT provides a dedicated area for employees to store their data either on a server (Courthouse, Sheriff's Office, County of Howard Office Building), or a designated folder on a designated computer (JP's and Precincts). These folders will be backed up to the IT backup system nightly.

IT holds backups for about 90 days. However the amount of time the data is held varies by the amount of data vs storage available.

IT is NOT responsible for loss of any data that is not stored in the designated areas.

6.6 Cloud Storage

Any data owned by Howard County that will be stored in any Cloud environment MUST be stored in their county One Drive account.

7 Security

Howard County has a comprehensive computing environment that encompasses a broad array of networking, server and desktop computing platforms as well as the complimentary systems software. Users should never consider electronic communications to be either private or secure. E-mail and data could potentially be stored indefinitely on any number of computers, in addition to that of the recipient. Copies of email messages or altered messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to nonexistent or incorrect user names may be delivered to persons that the sender never intended.

Each User is responsible for ensuring that his or her use of outside computer and networks, such as the Internet, does not compromise the security of Howard County's computer network. This duty includes taking reasonable precautions to prevent others from accessing the County's network without authorization and to prevent introduction and spread of viruses.

7.1 Network / Internet Security

Standards and requirements exist to ensure security and availability of the data and systems. The County's network connects to the Internet through a firewall and Intrusion Prevention System (IPS).

The County also employs a web content filtering system in an effort to ensure that county internet resources are not being mis-used. Examples of mis-use would be visiting websites for extended periods of time, or repeatedly that have no value to the operation of business activities of Howard County. There are some sites that will be blocked by the I.T. Director whenever use of those sites is felt to have a negative influence on employee performance by a department head. Department heads can request that sites become black-listed to the I.T. director and he shall make every effort to investigate the feasibility of such a block.

At times there will be other technology that will be employed by other departments for the operation of that department. It is the I.T. Department's responsibility to ensure network security at all times. It is suggested that before ANY technology is connected to the County's network, that was not procured by the I.T Department, the I.T. Director should be contacted and be present at any meetings with the vendor prior to purchasing and installation of said technology, in the interest of network security. Failure to follow this guideline can result in denial of installation of said equipment / software.

Security Patches -The County has a process to update all computers with the latest security patches to enhance security. The application vendors should adhere to the industry practice of compliance to the latest version of system software levels to ensure maximum security to information and services provided by the County.

Network Devices – 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 Howard County access to any computer or private network connection.***

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

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

To maintain the security of the County network, all the Virtual Private Network (VPN) Users should ensure that:

- Their County PC has the most current virus protection installed • Operating system has all the recommended patches installed • Browsers have all the recommended patches installed.

Security Issues – The Howard County Information Technology department has several levels of potential security related issues, such as security breaches, or violations, that should all be handled in the appropriate manner according to severity.

- **Level I Incident** o User feels that their user name and password have been compromised and feel that an un-authorized person can gain access to the County's computer system with their account.

- Suspected sharing of user account information with other users and or non-employees • **Level II Incident**
  - Involuntary employee termination ○ Employee arrest
- **Level III Incident** ○ Suspected Computer break-in or computer virus ○ Loss or suspected compromise of VPN password
  - Physical Intrusion (unauthorized entry of both criminal and non-criminal type) ○ Disaster or any form of major damage at computer site (Howard County Courthouse Data Processing Room and Howard County Sheriff Office) ○ Sudden employee resignation.

Actions to take upon level of severity – The following should be followed upon learning of a security issue guided by the severity set forth above.

- **Level I Incident –** Notify the Howard County Information Technology Department within one working day of the suspected violation. The IT department will then determine the action required, if any, from the user.
- **Level II Incident** – Notify the IT Department and District Attorney's Office within one hour of the security issue, at which time the IT staff will take appropriate actions to suspend or terminate the user's account.
- **Level III Incident** – Notify the IT Department immediately of the incident, regardless of time of day, by the appropriate means of contact. The IT staff will then immediately rectify the situation or respond to the location the issue occurred at.

The I.T. director, may, at his discretion remove computer access from any user account that could potentially constitute a security breach of the Howard County System for any of the above reasons 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.)

If contact cannot be made with the IT director, contact the Howard County Sheriff's Department, who will at all times, have contact with the IT director or IT Technician for Level III incidents.

7.2 Anti-Virus Protection

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

In some cases, simply reading an e-mail 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 e-mail and attempt to intercept viruses. However, no safeguard is foolproof, and viruses can find their way into County Users' computers from a variety of other ways (e.g., USB drives, internet file transfer, etc.). Each User is responsible for taking reasonable precautions to avoid introducing viruses into the County network, including but not limited to:

- Always run the County standard, supported anti-virus software that the County provides.
- NEVER open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- If you receive an email with an attachment from someone you know, verify the email and attachment is something you were expecting. If not then contact the sender to verify that the attachment was something they intended to send.
- Delete and never forward spam, chain, and other junk e-mail.
- Never download files from unknown or suspicious sources.

- Avoid USB drive sharing with read/write access unless there is absolutely a business requirement to do so.

Viruses and Laptops/Mobile Device

Viruses can gain back door entry via laptops and mobile devices that are normally outside the network and which may get infected. To eliminate such risks, the following guidelines should be used while using laptops on the County network.

1. Always make sure that you have current antivirus protection on the laptops. County provided laptops should have Bitdefender antivirus software on them. If it is not present, please contact IT.
2. If connected on the county network, the antivirus signature for this software is updated daily. All other county laptop Users should ensure that they periodically, (monthly) connect the laptops to the county's network overnight to get the signature updates.
3. Scan your hard disk periodically for any virus. Once a week is an ideal frequency as this would help the ongoing detection of any virus, or new virus, on your machine.
4. If required, IT will schedule a maintenance window with the department head to turn in their laptop to be scanned and updated.

Non-County laptops or mobile devices are not be connected to the County network. If it is totally unavoidable then the user must use the Guest Wifi Network.

Following these steps while using your laptop or mobile device will help ensure the safety and security of the County's data and network. For questions, please call the IT Department.

7.3 WIFI

Wireless access is available at multiple locations throughout the county. Sharing the Pre Shared Key to other people without authorization is prohibited.

Wireless access at the Justice of the Peace and Precinct Barns are designed for County Employee use only. Wireless access at the Sheriffs Office, Courthouse, and library are defined by two separate SSID's. All devices that need access to the wifi at these locations MUST be registered with the IT.
SSID HowCO is designed for county employees only that need to access the servers with their county owned laptop or tablet.
SSID Court_Public is designed for all other devices owned by County Employees, vendors, and guest that are working on location on behalf of Howard County.
Devices to be used on the HowCo and Court_Public network MUST be registered with IT prior to use.

7.4 Remote Access

Remote access is limited to employees authorized by their department heads and IT.

7.5 IDs & Passwords

Passwords are an important aspect of computer security. They are the front line of protection for User accounts. A poorly chosen password may result in the compromise of Howard County's entire corporate network. The scope of this policy includes all personnel, including third parties, who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Howard County facility, has access to the Howard County network, or stores any non-public Howard County information. As such, all are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Users are responsible for safeguarding their passwords for access to the computer system. Users are responsible for all transactions made using their passwords. No User may access the computer system using another User's password or account without express permission or portray oneself as another User.

In order to provide appropriate network security, this policy mandates that County IT utilize passwords and periodically require Users to select a new password, one that they have not used before. Although Users have confidential passwords, this should not be construed to mean that the application data is the property right of the User or that network, internet nor that e-mail access is for personal confidential communications or that the password is to protect the employee's privacy. Users are expected to follow these guidelines:

- Passwords shall remain confidential and should not be printed, stored online or given to others.
- Passwords are recommended to be changed every 90 days.
- Passwords shall be at least eight characters long.
- Passwords shall contain characters from at least three of the following four classes: (i) English upper case letters, A, B, (ii) English lower case letters, a, b, (iii) Westernized Arabic numerals, 0,1,2, and (iv) Non-alphanumeric ("special characters") such as punctuation symbols.
- Passwords may not contain your User name or any part of your full name.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication.
- The password shall not be a word found in a dictionary (English or foreign)
- The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters,
- 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.
- The password shall not be any of the above preceded or followed by a character (e.g., secret!, !secret).

7.6 Third Party Access

ALL Third-party access, or outside consultants MUST be approved by the IT Director of Howard County, before access is granted.

7.7 Desktop Security

Please follow the guidelines below to avoid security breaches:

- Close sensitive or confidential applications and lock your workstation when you leave your desk.
- Do not leave portable media unattended such as CDs or USB drives.
- Log off or lock your computer when you leave for extended periods.
- Never write your passwords on a sticky note nor try to hide them anywhere in your office.
- Remove printouts from printers before leaving your office.
- Shred sensitive printouts or paper when you are done with them.
- Where appropriate: o Use a screen filter to minimize the viewing angle on a computer monitor.
  o Enable a password-protected screen saver. (Must be disabled for technical support.) o Clear cache files on computer and memory on devices like printers regularly.

7.8 Backup Policy

All back ups are done by the Microsoft Cloud and there is a 5-year retention policy for all data.

7.9 Computer Data Backup

For all servers in the county's data center in the Courthouse, the following backup policy is administered.

Full Backup: Every day each vital server is backed up. This includes the application files and data files. Individual work stations are not backed up. A Master is performed with incremental forever. However a new master is created at random intervals for backup cleanup. Backups occur at night so any new data lost between backups can not be recovered.

Retention Policy: Backups are retained for a 30 days duration.

User Data Backup: All users of the County network are allocated a network share drive that will be connected as the I:\ Drive, J:\ Drive or K:\ Drive on your computer under the My Computer option. The IT Department has allocated the network drives to safeguard all electronic property of the county and to allow users to quickly recover from a crashed computer by not having their data located directly on their computer. Users are STRONGLY encouraged to participate in this method of document storage.

7.10 Security Access Removal

Computer System Security: Department heads shall notify IT immediately of when a user is or will be terminated so their computer and email account can be deactivated. Terminated employees email will be archived off the server for 3 years before deletion unless the department head request something different.

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

7.11 Retirement/Destruction

All computers, network equipment, and peripherals replaced will be reviewed to see if it can be recycled for County use or if it must be retired. The recycling of a device is determined on whether it will support the current operating system and run without error.

All computers that are brought into IT will have the hard drive removed and held for a minimum of 90 days. This includes SSD drives, mechanical drives, and M.2 Storage devices. After 90 days if the drive can be reused then it will be formatted and held as a spare. If the drive is an obsolete drive then it will be destroyed.

7.12 Related Laws and Statutes

The State of Texas has established laws relating to computer and electronic security and crimes related thereto. Texas Penal Code Chapter 33 details the definitions, offenses, and penalties for computer crimes committed in the State of Texas. All logged computer transactions are logged by a user's access credentials, (username / password). Users of the County network are advised to NOT give ANYONE their password or username for security of the county network, and to protect the user. Different users inside departments may have different levels of access to the computer system, and by sharing their password to someone who may not have the same access, a security risk is introduced, and possible violation of criminal / civil law may occur.
Texas Penal Code Chapter 16 relates to the interception of electronic communications including telephone "tapping", interaction of electronic mail (e-mail), interception of telephone calls, and disclosure of said information.

8 Weather Emergencies and 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.

- All computer equipment should be powered off. This applies to personal computers; workstations, printers and any associated peripheral devices (i.e., scanners, etc.). After powering down the equipment, disconnect the power cables from the receptacles to protect equipment from potential surges from lightning.
- Any equipment located on the floor should be moved to a higher location and away from any windows. All monitors should be turned so that no screens face the direction of 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.

9 Policy Infraction

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 Howard County to handle infractions as follows:

1. The violation shall be reported to the User's supervisor or manager.
2. The supervisor may discipline the User as supervisor deems appropriate, but shall 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 "*Howard County Personnel Policies and Procedures*."

10 Computer Support / Technology Requests

10.1 Help Desk

Information Technology Services offers support for existing County computer systems by calling a local number during business hours, 8:00am-5:00pm, Monday through Friday. For those departments that require 24/7 support, (Sheriff and Emergency Services), cell phone numbers have been provided.

11 Definitions

- Attachments - Files created in other applications (such as Word, Excel).
- E-Mail - An electronically transmitted message, along with any attachments and any information appended by the e-mail system.

- E-Mail System - Computer hardware and software system that allows personal computer users to send, receive and store messages, documents and files with other individuals or groups of people over an internal network or the Internet.
- Employee – Any person who is currently on the Howard County payroll and works in a county office. Any elected or appointed County official. Can be full-time (40 work hours in a week) or part-time (less then 40 hours in a week).
- Encryption - A means of coding messages so they appear to be random characters. Encryption has two benefIT. First, it prevents disclosure of sensitive information to unauthorized third parties. Second, encryption allows for "authentication" of the information sent.
- Freeware - programming that is offered at no cost, which is copyrighted so that one can't incorporate IT programming into anything one may be developing.
- Hacking – the unauthorized attempt or entry into any other computer or system.
- Internet – a world wide computer network through which you can send a letter, chat to people electronically or search for information on almost any subject you care to think of. Quite simply it is a "network of computer networks".
- Internet Browser - an application that displays HTML and other information found on the Internet. Netscape Communicator, Internet Explorer, and Mosaic are examples of browsers. This type of client software accesses the World Wide Web and Gopher services and lets you drift from link to link without having to have a purposeful search.
- Internet Service Provider (ISP) - an entity that charges startup and monthly fees to users and provides them with the initial host connection to the rest of the Internet usually via a dialup connection.
- Intrusion Alarm System – An electronic system that is designed to detect unauthorized entry into a building or secure location during a set time period and to report any unauthorized entry to the appropriate authority.
- IT - Information Technology Services Departmental label referring to the employees of Howard County Information Technology and current information technology outsource vendor.
- Panic System - A system installed that is used to immediately report danger or request officer assistance due to an unforeseen or unknown situation. The panic system is created utilizing wireless "pendant" panic buttons that, when activated, cause a pre-recorded message to broadcast over the Howard County Sheriff's Department main radio channel.
- Public Record – as defined in Texas Open Records Act.
- Public Resource - Includes not only County equipment, hardware, software or tangible articles, but also the employee's time expended while on duty with the County.
- Risk - Those factors that could affect confidentiality, availability, and integrity of Howard County's key information assets and systems. Howard County is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.
- Shareware - software that is distributed free on a "trial basis" with the understanding that the user may need to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date (after 30 days, the user can no longer get access to the program). Other shareware (sometimes called liteware) is offered with certain capabilities disabled as an enticement to buy the complete version of the program.
- Third Party – Any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.
- Trade Secret – as defined by law.
- World Wide Web (WWW) - a hypertext-based distributed information system for linking databases, servers, and pages of information available across the Internet.

RELEVANT PENAL CODE AND OTHER STATUTES

1.) Texas Penal Code CHAPTER 33. COMPUTER CRIMES

2.) Texas Penal Code CHAPTER 16. CRIMINAL INSTRUMENTS, INTERCEPTION OF WIRE OR ORAL COMMUNICATION, AND INSTALLATION OF TRACKING DEVICE

3.) USC – Electronic Communications Privacy Act

4.) Other related State and Federal Law

5.) CJIS Security Policy Manual dated: April 2007 (Version 4.4)

12 Signature of Agreement

I, _____ have read and agree to abide by the Technology Usage Policy while employed, affiliated with, or doing business with Howard County.

Signature: _____ Date: _____