

20226

SUBJECT: GENERAL GUIDELINES

TITLE: COMPUTER POLICY

Modified
Removed
Added

I. PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at all Hunt County facilities. The rules described in this policy are in place to protect Hunt County. Inappropriate use exposes Hunt County to unnecessary risks, which include but are not limited to virus attacks, compromised network systems and services, and legal issues.

II. SCOPE

This policy applies to all employees, vendors, contractors, consultants, temporary employees, and all other workers at Hunt County. This policy applies to all personnel affiliated with third parties. This policy applies to all equipment owned or leased by Hunt County.

III. BACKGROUND

The Information Technology Department's intention for publishing this policy is not to impose restrictions that are contrary to Hunt County's established culture of trust and integrity. The Hunt County Information Technology Department is committed to protecting the county, its employees, and our partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every Hunt County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

IV. POLICY

General Policy

It is the responsibility of the individual employee to read, understand, and abide by this and other policies regarding the usage of Hunt County Information Technology Systems.

While Hunt County Information Technology Department desires to provide a reasonable level of privacy, users should be aware that the data they create on Hunt County systems remains the property of Hunt County. Because of the need to manage and protect the county's systems and network, Information Technology cannot guarantee the confidentiality of the information stored on any network device belonging to the county. Additionally, all county data may be subject to open records request. ~~request including personal data that is stored on county systems.~~

request including personal
at 12:30 o'clock p M
JUL 31 2026
BECKY LANDRUM
County Clerk, Hunt County, Tex.
by

For security and network maintenance purposes, authorized individuals within Hunt County may monitor equipment, systems and network traffic at any time.

The use of Hunt County automation systems including computers, laptops, mobile devices, fax machines, servers, databases and all forms of internet access is strictly for authorized county business and purposes only.

The same standards of decorum, respect, and professionalism that guide us in the office environment apply to electronic communications with third parties. Important, confidential, and proprietary information is stored on county computer systems, thus only Hunt County personnel are allowed access to the county's computer systems.

All computer information is considered confidential unless otherwise specified. Accessing or attempting to access confidential data is strictly prohibited unless you have been specifically granted access to view it. Confidential information shall only be used for its intended purpose.

All information on user computers, network shares, databases, email, and other storage locations is considered Hunt County property. Deleting, altering, or sharing any confidential or proprietary information during employment or upon termination is a violation of state law and will be investigated and prosecuted.

Users of the email system are personally responsible, with guidance and training from your supervisor and Information Technology Department staff, to manage email messages as well as other electronic documents according to the county's retention policy and schedule. It is the responsibility of each employee to retain emails for the applicable records retention period. Retention periods are determined by the type of record or document to which the email relates. The email, including the sender, recipient, date and time sent, subject line, and any attachments, must be retained as part of the official record. As a best practice, employees should retain all non-spam emails unless they are specifically authorized for deletion under Hunt County's approved Records Retention Schedule.

Use of Hunt County computers, networks, email, and internet is a privilege and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to the following:

1. Leaving passwords visible to anyone other than yourself or deliberately sharing your passwords, whether on paper, computer, or mobile device.
2. Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial email ("spam") that is unrelated to legitimate county purposes.
3. Engaging in private or personal business activities, including excessive personal use of Hunt County email.

4. Using someone else's credentials to access CJI data, courts and justice software, networks, servers, drives, folders, or files to which the employee has not been granted access or authorization.
5. Making unauthorized copies of county data.
6. Destroying, deleting, erasing, concealing county data, or otherwise making files or data unavailable/inaccessible to the county or to other authorized users of county systems.
7. Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way.
8. Engaging in unlawful or malicious activities.
9. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code/file designed to disrupt, disable, impair, or otherwise harm Hunt County's network or computer systems.
10. Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages.
11. Sending, receiving, or accessing pornographic materials.
12. Causing congestion, disruption, disablement, alteration, or impairment of Hunt County networks or systems.
13. Failing to log off any computer or any other form of electronic data system to which you are assigned, if you leave such computer or system unattended.
14. Defeating or attempting to defeat security restrictions on Hunt County systems and applications.
15. Installing software of any kind on Hunt County systems without authorization from the Information Technology Department.
16. Removing any Hunt County computer system from county premises, unless authorized by the Hunt County Information Technology Director and the proper paperwork is completed, *except for mobile systems that are issued to employees to utilize outside the normal operating hours.*

Internet Access

The internet is to be used to further Hunt County's mission, to provide effective service of the highest quality to the county's citizens and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the internet for professional activities and career development. The various modes of internet access are county resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Hunt County systems are allowed to access the internet only through county approved and secured internet accounts. Employees are strictly accountable for the content of their internet usage history and messages. Individuals shall in no way attempt to circumvent filters and other security measures restricting access to files, data, or networks.

Brief and occasional personal use of the email system or the internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the county or otherwise violate this policy.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the county business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

All information created via email, internet, network, or other means of official communication is the property of Hunt County. Employees should not have any expectation of privacy regarding such information. This includes all email messages and electronic files. At the direction of an elected official or department supervisor, the Hunt County Information Technology Department may, without prior notice, access, monitor, review, copy, or preserve messages, files, and other data stored on or transmitted through County-owned computer systems when necessary to support County operations, investigate policy violations, respond to legal requirements, or protect County information systems. When it is necessary, Hunt County may disclose text or images to law enforcement or other third parties without the employee's consent.

To minimize vulnerabilities on Hunt County computer systems, all downloaded files will be scanned with virus detection software before they are viewed or opened.

Employees may not use Hunt County systems or network for any of the following reasons:

1. Downloading of any software without the prior approval of Hunt County's Information Technology Department.
2. Dissemination or printing of copyrighted materials, including articles and software, in violation of copyright laws.
3. Operating a business, usurping business opportunities, soliciting money for personal gain, or searching for jobs (excluding searching for other jobs within Hunt County offices or departments, which is permitted).
4. Offensive, harassing statements or language including disparagement of others based on their race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.
5. Sending or soliciting sexually oriented messages or images.
6. Visiting sites featuring pornography, terrorism, espionage, theft or drugs.
Exceptions for criminal investigation purposes only.
7. Gambling or engaging in any other activity in violation of local, state or federal law.
8. Unethical activities or content, or activities or content that could damage Hunt County's professional reputation.
9. ***Exceptions to the above conditions will apply to the departments that require full access to the internet for job related reasons. A request to gain access to other internet sites must be provided by the department head or elected official.***

The Hunt County website is a useful tool that provides a means for departments to communicate and provide services to the citizens of our county. Departments can establish and maintain a department webpage within the county web site. Departments are responsible for ensuring that the content will be reviewed, approved and published to the production web site by the Information Technology Department.

Network and Systems Authentication

To maintain the security of Hunt County's network infrastructure, the Information Technology Department provides every employee with a unique username and password for email, domain computers, courts and justice software, and various other network and software applications.

Each computer user is granted distinct permission based on the requirements of their specific position in Hunt County. If a user cannot access specific data on a computer, server, or courts and justice software, that user's supervisor must request access on their behalf via the correct form provided by the Information Technology Department.

A Hunt County computer user's password must meet the minimum password complexity requirements as determined by the Hunt County Information Technology Department. Minimum password complexity requirements are determined by the ease and ability of current hackers to circumvent passwords. The current complexity requirements may increase over time as technology advances.

Minimum password complexity requirements:

1. Must not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
2. Must be at least twelve characters in length.
3. Must contain characters from each of the following four categories:
 - a. English uppercase characters (A through Z)
 - b. English lowercase characters (a through z)
 - c. Base 10 digits (0 through 9)
 - d. Non-alphanumeric characters (for example, !, \$, #, %)

Multi-Factor Authentication (MFA)

The purpose of MFA is to protect Hunt County information systems and reduce targeted cyberattacks. To ensure the security and compliance of Hunt County data and resources, all employees are required to maintain the MFA method assigned to them. MFA methods may be modified depending on the requirements of the position held.

Multi-factor authentication (MFA): Using two or more factors to validate the identity of a user.

There are five factor types used in combination resulting in multi-factor authentication:

1. Something the user knows (username and password)
2. Something the user has (an item the user physically carries with them) for example; mobile phone or any other electronic device (hardware token).
3. Something the user is (biometrics: fingerprints, face scan, etc.)
4. Somewhere the user is (geolocation, on premises)
5. Something the user does (keystroke patterns)

Scope:

This policy applies to all individuals and entities, including but not limited to employees, affiliates, vendors, retired employees, and volunteers, that connect to or otherwise utilize Hunt County's network or technology resources. This policy applies to any system accessing Hunt County data where MFA can be utilized.

Responsibilities:

Microsoft Authenticator app is the recommended MFA method and the official Hunt County method of MFA; it is a requirement for employees accessing Hunt County managed Microsoft resources such as Outlook, OneDrive, Word, and Excel.

In areas where mobile devices are prohibited, employees will be assigned a hardware token (physical device) to complete MFA. Failure to do so will result in loss of access to Hunt County systems until the token is recovered or replaced.

Employees are responsible for maintaining access to their registered Microsoft Authenticator application and must notify the Information Technology Department immediately if their mobile device is lost, replaced, or otherwise unavailable so that MFA can be re-established. Failure to enroll in or maintain the required MFA method may result in delayed account activation, restricted access to Hunt County systems, or suspension of access until compliance is achieved. It is the employee's responsibility to safeguard and retain assigned MFA hardware tokens where mobile devices are prohibited.

Enforcement:

This policy regulates the use of all MFA for access to Hunt County resources. Users must comply with this policy. Services will be disabled immediately if any suspicious activity is observed, and services will remain disabled until the issue has been identified and resolved to the satisfaction of the Hunt County Information Technology department. Any individual or entity found intentionally violating this policy will be subject to disciplinary action.

Legacy MFA:

To strengthen the security of Hunt County information systems, legacy multi-factor authentication methods, including SMS (text message) and voice call verification, cannot be used for Hunt County accounts.

SMS and voice call authentication methods provide a lower level of protection against modern cyber threats, including phishing, SIM-swapping, and social engineering attacks. Microsoft Authenticator provides a more secure method of verifying user identity and is the required multi-factor authentication method for all Hunt County employees, unless your supervisor prohibits mobile device usage. Alternate secure methods of MFA will be provided in this instance.

AI Usage:

Employees shall not enter, upload, or disclose confidential, sensitive, or non-public County information into any public or unapproved AI system. This includes, but is not limited to, personally identifiable information (PII), criminal justice information (CJI), protected health information (PHI/HIPAA), financial information, passwords, or other sensitive Hunt County data.

The Hunt County Information Technology Department reserves the right to restrict or prohibit the use of AI applications that present security, privacy, or operational risks to Hunt County information systems or data.

Failure to comply with this policy may result in disciplinary action, up to and including the loss of access to County technology resources or other disciplinary measures as deemed appropriate by Hunt County.

Security Awareness and AI Training

Hunt County requires all new employees to complete the provided cyber security and AI training course within 24 hours of gaining access to the Hunt County computer network system, *exceptions for employees that will never use a computer in the course of their employment*. Individuals that will access Hunt County's courts and justice software may be subject to completing CJIS Security Awareness Training as detailed in the U.S. Department of Justice Criminal Justice Information Services (CJIS) Security Policy **Version 6.0**. Access may be revoked for failure to complete the required training.

Personal Electronic Equipment

Hunt County prohibits the use of any type of camera phone, digital camera, video camera, or other form of image or voice-recording device without the management permission to record, photograph or download any file, software, confidential information, or County-owned information. This provision does not apply to designated county personnel who must use such devices in executing their duties of their positions.

Employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, flash drives, tablets, or other data storage media) to the workplace or connect them to county electronic systems unless expressly permitted to do so by management. Any employee bringing a personal computing device, data storage device, or image-recording device onto county premises thereby gives permission to the county to inspect the personal device at any time with personnel of the county's choosing, and to analyze any files, other data, or data storage devices or media that may be within or connectable to the personal device in question. Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not bring such items into workplace.

Licenses

Hunt County does not condone the illegal duplication of software or other copyrighted material.

Hunt County purchases and licenses the use of computer software from a variety of outside companies. Hunt County does not own the copyright to this software or its related documentation, and unless authorized by the software developer, does not have the right to reproduce it for use on more than one computer. Regarding the use on local area networks or on multiple machines, employees shall use software only in accordance with the license agreement.

Hunt County software licenses shall not be used for personal use on non-county computer equipment.

Software licenses purchased or received by employees for personal use are prohibited on Hunt County equipment.

Hunt County Information Technology Department is authorized to conduct random software license audits of its network and systems. Information Technology personnel shall install and/or relocate all computer equipment and software unless the employee is specifically authorized.

According to the U.S. Copyright Law, persons responsible for illegal reproduction of software can be subject to civil damages up to \$100,000 per work copied and criminal penalties including fines and imprisonment. County employees who make, acquire, or use unauthorized copies of software will be subject to the above law.

User Responsibilities

Computer users are responsible for the appropriate use of Hunt County computers and for taking reasonable precautions to secure the information and equipment entrusted to them.

Employees are responsible for reporting inappropriate use of Hunt County computers and breaches of computer security and assisting in resolving such matters.

Any employee who learns of a violation of this policy should notify the appropriate Hunt County elected official, department head, or the Information Technology Department.

Again, it is the responsibility of the individual employee to read, understand, and abide by this and other policies regarding the usage of Hunt County Information Technology systems.

History

Created 07/07/2020

Modified 07/29/2026