CALHOUN COUNTY
BOARD OF COMMISSIONERS
POLICY STATEMENT

SUBJECT:	**DATE APPROVED:**	**EFFECTIVE:** Immediately	**POLICY NO.** 435
INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY	4/14/2020	**REPLACES:** #435 (3/16/00) and #440 (03/16/00)	

I. **PURPOSE:** Calhoun County provides information technology access and systems for the purpose of conducting official County business and the efficient exchange of information. These systems are necessary to meet the County's statutory and regulatory requirements, missions, goals, and other initiatives. As such, this technology must be managed responsibly to maintain the confidentiality, integrity, legality, and the availability of its information assets. This policy outlines the requirements and guidelines for acceptable use of Calhoun County information technology.

II. **AUTHORITY:** The Calhoun County Board of Commissioners authorizes the use of information technology systems for conducting County business and reserves the right to modify this policy at any time and for any reason.

III. **RESPONSIBILITY:** The Administrator/Controller or designee is responsible for administration of this policy. Users of County information technology systems are responsible for utilizing technology in an ethical, professional, and productive manner as necessary to conduct the business and activities of Calhoun County.

IV. **SCOPE:** This policy applies to every individual that is provided access to Calhoun County information technology, including, but not limited to, all employees regardless of status, elected officials, contractors, consultants, vendors, personnel affiliated with third parties, interns, volunteers, and temporary workers. Information Technology refers to the development, maintenance, and use of computer systems and software. For purposes of this policy, it includes all computer resources used by Calhoun County to create, store, retrieve, transmit, and manipulate data or information, including but not limited to, computer equipment, software, operating systems, data storage, network accounts, electronic communications, internet, web browsing, social media, and voice and video equipment/systems. This policy applies to all computer and network resources leased, owned, or managed by Calhoun County, as well as all electronic communications and information contained within the systems/equipment.

V. **POLICY:**

A. General Use and Requirements:

1. Under the direction of the Administrator/Controller or designee, the information technology systems of the County shall be managed by the IT Department including

the responsibility for ensuring the safety, security, and integrity of County owned technology and resources.

2. Users of Calhoun County information technology are responsible for exercising good judgment regarding appropriate use of Calhoun County resources in accordance with County policies, standards, and guidelines.

3. All information used, created, sent, stored, or retrieved with County provided technology is the property of Calhoun County, and may be accessed or monitored at any time, and for any reason. For County departments utilizing confidential or protected information, access or monitoring will only occur based upon a good faith belief that there has been a violation of this policy and/or law.

4. Depending on the content, all information used, created, sent, stored, or retrieved with County provided technology is subject to the right of discovery in legal actions against the County and may be subject to the Freedom of Information Act and other disclosure, without notification and/or consent of the user.

5. Any communication or information transmitted or received via County provided information technology is subject to the interception and/or receipt by another employee authorized by the Administrator/Controller or designee. As such, there should be no expectation of user privacy as it relates to the use of County provided information technology, except as otherwise protected or restricted by law. The County discloses that it reserves and may, from time to time, exercise the right to review, audit, intercept, access and/or disclose all matters contained in the County's Information Technology system at any time, with or without notice to an authorized user.

6. Employees must use only software that is authorized by the County on County computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on County computers must be approved and installed by the County IT Department.

7. Authorized users of portable devices, such as laptops, tablets, and smartphones, are responsible for safeguarding these devices from being lost or stolen. Portable devices must be kept in a safe and secure area to avoid damage or access by unauthorized user(s).

8. Information that has been deleted by the user from the County information technology systems may be backed-up and retrieved by the County. The IT Department may also conduct random audits to ensure proper use of all technology related resources.

9. Authorized users must immediately notify their supervisor, Department Head/Elected Official, or the IT Department if they become aware of any violations of this policy.

B. Authorized Users:

1. Authorized users shall be defined as anyone that has been provided Calhoun County information technology access as part of their job or work function, including, but not limited to, all employees regardless of status, elected officials, contractors, consultants, personnel affiliated with third parties, as well as temporary workers.

2. The IT Department shall be responsible for the development and implementation of the processes and procedures required for authorizing users and shall provide final approval for all authorized users prior to granting access to any County information technology.

3. Department Heads and Elected Officials, or designees, shall comply with the processes and procedures developed by the IT Department that are necessary to approve and grant access to County information technology authorized users, and will help to ensure the safety and security of the systems being utilized.

4. Authorized users are expected to use County provided information technology for the performance of work and conducting the day-to-day business activities of the County in a productive manner. Any personal use must be kept to a minimum and is also subject to the approval of the applicable Department Head or Elected Official.

5. Authorized users that have been granted a username and password needed to access information technology systems or software are responsible for protecting the information and shall not reveal or share it with others, including co-workers. The requirement and utilization of a user name or password does not restrict the right of the County to access the information on its systems.

6. All authorized users of the County e-mail system must establish a signature line below the bottom of every message that prominently states, "This message has been prepared on resources owned by Calhoun County, Michigan. It is subject to the Information Technology Acceptable Use Policy of Calhoun County." The signature line must also include the user's name, department, and telephone number.

7. Questions regarding the appropriate use of Calhoun County information technology should be directed to an employee's supervisor, the applicable Department Head/Elected Official, or the IT department.

8. The authorization to use County provided information technology may be restricted, suspended, or revoked at any time due to operational or business needs, protection of County assets or resources, or for use that is inconsistent with the established procedures and standards of this policy.

C. Prohibited Uses

The activities in the following section are, in general, prohibited. Users may request a waiver to be exempted from these restrictions during the course of their legitimate job responsibilities. Prohibited Uses of County information technology (including but not limited to):

1. Employees may not use the County's Internet, e-mail, or other electronic communications to transmit, retrieve, or store any communications or other content of a defamatory, discriminatory, harassing, or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference may be transmitted. Harassment of any kind is prohibited. Disparaging, abusive, profane, or offensive language and any illegal activities, including: piracy, hacking, extortion, blackmail, copyright infringement, and unauthorized access to any computers on the Internet or e-mail are forbidden.

2. Use of the County internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's job performance, is not detrimental to the County in any way, not in breach of any term and condition of employment, and does not place the individual or the County in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

3. Use of streaming video, such as YouTube, unless related to County business or otherwise approved by the employee’s supervisor.

4. Use of the internet or email to make personal gains or conduct a personal business.

5. Use of the internet or email for gambling, betting pools, pyramiding schemes, chain letters, or investment clubs.

6. Circumvention or violation of the Open Meetings Act.

7. Solicitation and/or fundraising that has not been pre-approved.

8. Lobbying or use for political purposes/campaigns.

9. Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software, including, but not limited to; the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by the County.

10. Revealing a User’s or another user’s account password to others or allowing use of your account by others. This includes, but is not limited to, family and other household members when work is being done at home.

11. Intentionally introducing malicious code, including, but not limited to; viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

12. Creating or attempting to create security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to; network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

13. Executing any form of network monitoring which will intercept data, unless this activity is part of the User's normal job/duty.

14. Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

15. Engaging in any activity that is illegal under local, state, federal or international law while utilizing County owned resources.

16. Engaging in any blogging or social media posting that may harm or tarnish the image, reputation, and/or goodwill of the County and/or any of its Users. Users are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by the County. Authorized users are strictly prohibited from downloading/installing/using any Instant Messaging (IM) software without specific authorization in writing from their respective Department Director and the Information Technology Department. See Social Media Policy #430 for additional requirements for the use of Social Media.

17. Violation(s) of any other County policy in the use of information technology, including but not limited to: Policy #286 Anti- Fraud, Policy #290 Workplace Violence, Policy #315 Equal Employment Opportunity, and Policy #326 Harassment, and Policy #430 Social Media.

D. User Security

1. Authorized users are responsible for their individual computer accounts and shall take all reasonable precautions to prevent others from using their accounts. All PCs, notebooks, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less. Authorized users without a password protected screensaver shall log off each time they leave the computer unattended. All authorized users will log off at the end of their work shift unless instructed otherwise. Account owners are ultimately responsible for all activity under their account.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

3. Users must exercise extreme caution when opening e-mail attachments received from unknown senders. These may contain malware or viruses. If in doubt, a User should request assistance from IT staff.

4. Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

5. Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only County authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

F. Authorized User Administration

1. Compliance measurement - The IT Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, and internal and external audits.

2. Before receiving access to any County system, each authorized user shall sign an acknowledgement statement certifying that he/she has read and understand this policy, and that he/she will abide by the provisions contained herein.

3. Any exceptions to the policy must be approved by the IT Department and Department Head or Elected Official for whom the User works.

4. All materials sent or received using the County information systems shall be considered property of the County. An authorized user does not have privacy rights in any matter created, received or sent. The County reserves the right to monitor, access, or disclose any message created, received, or sent via the Internet or e-mail at any time, without advanced notice.

5. Electronic messaging systems, as well as other computer systems, are subject to the right of discovery in legal actions brought against the County. Additionally, electronic messages may be subject to disclosure under the Freedom of Information Act.

6. The County reserves the right to audit networks, systems, and computers on a periodic basis to ensure compliance with this policy. Users should have no expectation of privacy in personal materials stored, whether incidentally or intentionally, on the County's systems. At the discretion of the County, materials may be examined internally or disclosed to third parties, and except as required by law, the County assumes no specific duty to inform Users how their personal data transmitted or stored on County systems is stored, backed up, deleted, examined, or disclosed.

7. All County data or intellectual property developed or gained during the period of employment remains the property of the County and must not be retained beyond termination or reused for any other purpose.

8. All County equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices, and CDs/DVDs, must be returned to the County at termination of employment.

G. Violations:

1. This policy must be followed in conjunction with other County policies governing appropriate workplace conduct and behavior. Any violations or abuse of this policy by employees may be denied future access and, if appropriate, be subject to disciplinary action, up to and including termination of employment.

2. Violations of the rules set forth in this policy by the general public as it relates to use of the County website, e-mail, and/or social media, may result in restricted or terminated access depending on the circumstances.

3. The County may initiate legal action for violations as appropriate. Law enforcement personnel may also be notified when criminal activity is suspected.

VI. **SUMMARY**: This policy is established to ensure the safety, security, and integrity of Calhoun County information technology. It is designed to provide the terms and conditions for appropriate access and use necessary for conducting official County business, and for the efficient and professional exchange of information.