ANTRIM COUNTY
Acceptable Use of Information Technology Policy
Adopted: April 12, 2018

1.0 Objective

This policy identifies acceptable use of information technology resources (IT Resources) to conduct county business and provides notice of expected User behavior. Unacceptable IT Resource use exposes the county to unwarranted risks, such as data breach, disruption of county network or application services, and other legal and liability issues. Unacceptable use may also consume IT Resource capacity and hinder county employees' ability to conduct business.

2.0 Scope

This policy applies to all users granted access rights to county IT Resources (Users).

3.0 Policy and Procedures

3.1 Acceptable Use of IT Resources

IT Resources, including devices, networks, data, software, email, and system accounts, are provided to conduct official county business. Authorized Users must act within the scope of their employment, contractual, or other relationship with the county and must agree to use IT Resources efficiently, responsibly, professionally, ethically, and lawfully, using approved applications, tools, and mechanisms. Users, regardless of their relationship with the county, as a condition of receiving access to county IT Resources, agree to abide by this standard, all applicable county policies and procedures, and all federal, state, and local laws.

Users must review these guidelines regularly. Failure to do so does not justify non-compliance.

3.2 Unacceptable Use of IT Resources

3.2.1 Illegal Use

IT Resources may only be used for lawful purposes. Prohibited activity includes use that is illegal under local, state, or federal law; violates other applicable regulations, policies, or standards; compromises public safety or the privacy of legally protected personal information; is malicious; or is fraudulent.

Users must abide by all intellectual property laws. Downloading, duplicating, or distributing copyrighted materials without specific written permission of the copyright owner is not allowed. Users shall respect all licensing agreements.

3.2.2 Abuse

IT Resource use interfering with work obligations or county business is prohibited. IT Resources shall not be used for purposes unrelated to the county's business, unless specifically authorized. Examples of inappropriate use include:

- For commercial or personal product advertisements, solicitations, promotions, or for-profit purposes; political fundraising or lobbying; promoting a social, religious, or political cause; or gambling, gaming, or online shopping.
- To access, send, receive, or store any obscene, pornographic, offensive, or excessively violent content.
- To send messages containing unwelcome advances, profanity, or discriminatory or harassing remarks.
- To send hate mail or chain mail.
- To download entertainment software, music, movies, television shows, video-sharing content, or other similar files.

Users shall not download or install any software (including shareware and freeware) unless authorized by the Information Technology Department (IT). No county-owned or county-licensed software may be installed, copied, or used on non-county equipment unless expressly approved by IT.

Users shall not divulge or release any confidential information to the public that is not available to members of the general public. This does not prohibit disclosing a violation or suspected violation unless otherwise prohibited.

Incidental personal use of IT Resources during lunch or break times may be authorized by supervisors, but shall not interfere or conflict with a User's work obligations or county business and must comply with all applicable county policies.

3.2.3 Social Networking

Users shall not misrepresent their relationship with the county, imply county endorsement of products or services of a non-county entity, or give the impression that they are representing, giving opinions, or speaking on behalf of the county, unless part of their legitimate job duties.

Users are responsible for any online activity conducted with county email addresses. Users must recognize that their county email address associates them with the county.

Some internet sites may impose Terms of Service agreements that are unacceptable to the county, such as indemnification clauses or agreements to be sued. When accessing these sites without specific county authorization, the User accepts such terms solely in a personal capacity and is personally and solely responsible for any legal claims arising from an agreement "signed" by clicking to agree on the terms of service.

3.2.4 Security

Users must follow all applicable security policies and standards and are responsible for the reasonable (1) physical security and protection of their IT Resources and devices and (2) protection and use of granted access. Users shall not reveal to or allow use of their accounts or passwords by others, including family members. Users shall not leave workstations, devices, or IT Resources unattended without engaging password protections.

Users must maintain the security of county data. Providing unauthorized persons any information that is sensitive or protected by law; unauthorized posting of county information to external newsgroups, bulletin boards, or other public forums; sharing personal information about another person unless part of legitimate job duties; and storing county information in public storage services without IT approval are prohibited.

Users also shall not:

- Interfere with the normal operation of any IT Resource.
- Act to disrupt systems or cause unnecessary network congestion or application delays.
- Try to compromise or cause intentional damage or loss to county systems or data.
- Modify or circumvent security safeguards or access controls.
- Use tools or utilities to reroute traffic on, scan, probe, or attack a network.
- Intercept or try to intercept any data transmissions without authorization.
- Use unauthorized peer-to-peer (P2P) networking, file sharing, instant messaging or Internet Relay Chat (IRC) applications or services.
- Forward county email messages to personal email accounts that would create unacceptable privacy, security, or compliance risks.

- Use any unauthorized remote control software, tools, or services on any internal or external devices or systems not set up by IT.
- Store county data in public storage services, unless approved by IT.
- Post county information to external newsgroups, bulletin boards, or other public forums, unless authorized.
- Send unsolicited email messages, including junk mail or other advertising material, to individuals who did not specifically request such material.
- Install or attach any unauthorized equipment to an IT Resource without approval of IT and the resource owner, (e.g., wireless access points, modems, disk drives, external hard drives, networking devices, personal mobile devices or computers, etc.). Unauthorized equipment will be confiscated.
- Intentionally modify, damage, or remove IT Resources owned by the county without authorization from IT and the IT Resource owner.
- Intentionally modify, disable, test, or circumvent any IT Resource security controls without authorization.
- Intentionally cause a security incident resulting in a loss of data confidentiality or integrity or a disruption or denial of availability.
- Circumvent user authentication or compromise the security of a host, network, or account.
- Seek or enable unauthorized access to any computer system, application or service.
- Intentionally seek information on, obtain copies of, or modify files, data, or passwords of other Users.
- Impersonate or fraudulently represent other Users on the network.
- Try to access any computer account or part of the county's network to which they are not authorized.
- Participate in activities that promote computer crime or misuse, including posting on internal or external sites; disclosing passwords, credit card, or account numbers; and revealing system vulnerabilities.
- Try to circumvent this standard by using anonymous proxies, software or hardware; use software or websites to hide Internet activity; or use devices or utilities to remove or camouflage information of evidentiary value.

3.3 No Presumption of Privacy

Data is a valuable county asset that must be protected. Any data Users create, store, process, or send using county IT Resources remains the property of the county. The county cannot guarantee the confidentiality or privacy of Users, unless applicable law provides differently. Users have no expectation of privacy in their use of county-provided email, instant messaging, computing equipment, Intranet or Internet access, or other county information systems.

The county may actively monitor IT Resources to ensure compliance with policy. This includes real-time monitoring of network traffic; the transfer of data created, sent, received or stored on IT Resources; and other monitoring and auditing the county may deem necessary.

The county blocks unauthorized internal and external traffic and services that may cause risk to IT Resources. Any evidence of illegal activity or unacceptable use discovered during monitoring or reviews may be provided to county management or law enforcement organizations.

Electronic records may also be available for public distribution under the Freedom of Information Act (FOIA).

The county may require Users to surrender to county authorities any IT Resources (county owned or personal) that have been used to conduct county business or on the county's network, in response to discovery orders from a court of law; information holds from the Prosecuting Attorney; acceptable use or cybersecurity-incident investigations; or FOIA Requests.

3.4 Inadvertent or Erroneous Use

Users inadvertently directed to a website that violates laws, regulations, polices or this standard may claim erroneous use by **immediately** reporting to managers when unintentional misuse occurs. Self-reporting is encouraged and may be done without consequence in demonstrated cases of inadvertent use.

3.5 Responsibilities

- Elected and appointed department heads shall communicate this standard to all Users under their supervision.
- The Administration Office will ensure that Users read and understand this standard, and develop processes to certify and document User acceptance.
- Users shall read this standard, understand its expectations, and follow its provisions. Each User shall acknowledge receipt of this standard and any department-specific addenda. Each User shall report all violations to their supervisor, who must report all violations to IT Department.
- Contract staff, vendors, volunteers, and others who use IT Resources shall follow and acknowledge awareness of this standard.
- Elected and appointed department heads shall require all Users under their supervision to read and acknowledge this standard and abide by its provisions.
- The Administration Office shall support elected and appointed department heads as needed in assuring awareness and enforcement of this standard.
- IT shall receive and document reports of suspected abuse from any source and respond as necessary. IT may supervise periodic system and network audits for abuse and compliance with this policy. IT shall report abuse to the County Administrator and appropriate law enforcement officials when appropriate. IT shall also assist in preserving digital forensic evidence.
- The Administration Office with the assistance of IT as necessary shall ensure that contracts obligate contractors to comply with all applicable IT policies, standards, and procedures and that appropriate compliance activities occur.

3.6 Effect

This standard sets minimum expectations for all county IT Resources. Individual county departments may implement policies on IT Resources consistent with this standard and may implement more restrictive standards on IT Resources with prior coordination with IT Department.

All employees must realize that misuse or abuse of IT Resources may lead to agency investigation and criminal, civil, or legal actions and discipline, up to and including discharge. IT Resources may be removed from a work area for analysis.

4.0 Review

The Information Technology Department shall review this policy as needed or at least once every 3 years.

Policy Replaced Upon Adoption of this Policy: Computer, Network System, and Internet Use Policy (adopted 2/7/2005, amended 7/9/2009)