Geauga County Automatic Data Processing Board
Department of Information Technology
Charles E. Walder, Chief Administrator

Geauga County Acceptable Use Policy

ADP-25-A-004

Classification Level: PUBLIC

Sec. 1.0 – Applicability

The scope of this policy applies to **all users of Geauga County IT resources**, including: (1) County government employees and officials; (2) IT professionals and administrators with elevated access privileges; (3) contractors, consultants, and third-party vendors who access County systems or data; and (4) members of the public who are authorized to use any County-provided technology resources or services. Each category of user is expected to understand and abide by this policy when accessing or using County IT assets.

Sec. 2.0 – Policy Information

Issued: 07/16/2025
Reviewed: 07/16/2025

Sec. 3.0 – Purpose

To establish clear guidelines for the acceptable and secure use of Geauga County's information technology assets. This policy is designed to protect the confidentiality, integrity, and availability of County data and systems by defining appropriate user behavior and security practices. It ensures compliance with applicable laws, regulations, and industry best practices – including alignment with relevant *Center for Internet Security (CIS) Critical Security Controls* – in order to minimize risks such as data breaches, unauthorized access, and misuse of resources. By following this policy, all users will help safeguard public trust in the County's IT infrastructure and services while enabling effective and efficient use of technology.

Sec. 4.0 – Authority

The Geauga County Automatic Data Processing (ADP) Board provides technology services to County agencies and other County partners in Geauga County, its sixteen townships, and municipalities in Northeast Ohio. Our services include hosting, network, telecommunications, desktop computing, project management, unified communications (e.g. email, calendaring, team collaboration), and information security.

ADP operates under the leadership of the Geauga County Auditor, Charles E. Walder, who also serves as the Chief Administrator of the Automatic Data Processing Board. The ADP Board is created by Ohio state statute and, as such, the ADP Board is a separate appointing authority governed by the laws of the State of Ohio. The policies issued under this authority apply to all users as defined in Sec. 1.0 and are enforceable under applicable law and County regulations.

Ohio Revised Code § 307.847 – ADP Board Authority

Geauga County's IT Acceptable Use Policy is grounded in the statutory authority of the County Automatic Data Processing Board ("ADP Board") as defined by Ohio Revised Code § 307.847. Under this law, the Board of County Commissioners may **"require the county automatic data processing board established under section 307.84 of the Revised Code to coordinate the management of information resources of the county, the records and information management operations of all county offices, and the various records and information technologies acquired and operated by county offices"**. In Geauga County, the Commissioners have done so by resolution, expanding the ADP Board's duties to encompass county-wide information technology **and** records management functions. Once these duties are expanded, additional officials are added to the Board's membership by law – specifically, **"the prosecuting attorney, county engineer, county coroner, sheriff, and a judge of the court of common pleas"** must be included on the ADP Board (with each allowed to send a representative). This ensures that all major county offices are represented in governing the county's IT and information management.

Importantly, when the ADP Board's role is expanded under R.C. 307.847, it effectively assumes the responsibilities of the county records commission and microfilming board. The statute specifies that **"the county automatic data processing board shall have the powers, duties, and functions of the county records commission as provided in section 149.38 of the Revised Code and the county microfilming board as provided in section 307.802 of the Revised Code"**. In other words, the ADP Board becomes the *de jure* records retention authority and microfilm oversight body for the county (except regarding the county hospital). All records, equipment, and personnel from those former bodies are transferred to the ADP Board's jurisdiction as of the effective date of the Commissioners' resolution. The ADP Board thus serves as the single entity coordinating **all** aspects of the country's information technology systems, records management, and data processing operations.

Scope of County Network and "County Office" Definition

Under R.C. 307.847, the policy's scope extends to the entire Geauga County information network and all users who are part of a "county office." The law defines "county office" broadly to include **"any officer, department, board, commission, agency, court, or other office of the county and the court of common pleas"**. In practical terms, this means every elected office, administrative department, and agency of Geauga County government – as well as the Common Pleas Court – is subject to the ADP Board's authority and thus governed by the Acceptable Use Policy. This comprehensive definition ensures that all components of county government that utilize the county's IT resources or data systems are covered by the same rules and oversight. The County's network and computing environment (the "information resources of the county") therefore encompasses all hardware, software, databases, communication systems, and records management systems used by these county offices.

ADP Board Powers and Responsibilities under ORC 307.847

Ohio law vests the ADP Board with robust powers to standardize and supervise county information technology procurement and usage. **After a resolution is adopted under R.C. 307.847, *"no county office shall purchase, lease, operate, or contract for the use of any automatic data processing equipment, software, or services; microfilming equipment or services; records center or archives facilities; or any other image processing or electronic data processing or record-keeping equipment, software, or services without prior approval of the [ADP] board"***. In other words, **any acquisition or use of computer systems, IT hardware, software applications, electronic recordkeeping systems, microfilm/imaging systems, or related services by a county office must be approved by the ADP Board in advance**. This statutory requirement is central to the Acceptable Use Policy: County officials and employees cannot unilaterally purchase or deploy technology that connects to county networks or handles county data without Board authorization. The ADP Board reviews and coordinates all such technological decisions to ensure compatibility, security, and cost-effectiveness across the county.

The ADP Board's purview includes not only approving purchases but also establishing and operating central IT facilities. Under R.C. 307.847(D), the Board **"may establish an automatic data processing center, microfilming center, records center, archives, and any other centralized or decentralized facilities it considers necessary to fulfill its duties"**, and **"[a]ny such centralized facilities shall be used by all county offices"**. This means the Board can create shared services (data centers, archives, etc.) that all departments are required to use, further standardizing the county's IT environment. The Geauga County Department of Advanced Technology and Applications (DATA) (which operates under the ADP Board's authority) thus provides centralized network infrastructure, storage, email, and other IT services to all county offices. By law, the County Auditor serves as the chief administrator of these facilities and is responsible for operational oversight and budgeting of the ADP operations (with an annual budget submitted to the Commissioners). The ADP Board's budget and any facilities or services it establishes are funded through the normal county budgeting process, requiring appropriation by the Board of Commissioners.

In carrying out its mandate, the ADP Board may also set internal policies, standards, and rules governing the use of IT resources. The statute explicitly provides that **"[t]he board may adopt such rules as it considers necessary for its operation, but no rule shall derogate the authority or responsibility of any county elected official."** In effect, the Board can promulgate IT standards, security policies, usage guidelines, and other regulations to ensure efficient and secure use of technology county-wide – as long as those rules do not infringe on the legal powers of an elected office. (For example, the Board could set a county password policy or data retention standard, but it cannot use a "rule" to take away an elected official's core statutory powers.) The law further states that the Board's rules *may* include any additional regulations or technical standards the Board deems necessary. All county personnel and offices are required to abide by the ADP Board's duly adopted policies – including this Acceptable Use Policy – pursuant to the Board's statutory authority. Notably, nothing in the Board's rules can override the requirements of state or federal law, and the statute confirms that no ADP rule can reduce an official's legal responsibilities. This ensures a balance between county-wide IT governance and the independence of elected offices.

Finally, R.C. 307.847 allows the ADP Board, with the Commissioners' approval, to extend its services to other public entities by contract. The Board is authorized to **"enter into a contract"** with other government units (municipalities, townships, school districts, library districts, other counties' agencies, etc.) to **"provide microfilming, automatic data processing, or other image processing or electronic data processing or record-keeping services"** to those entities. In such cases, the Board sets a schedule of charges for services, and any revenue is handled through the county's general fund. While this aspect primarily concerns external agency contracts rather than internal use, it underlines the Board's broad authority to act as a county IT service provider. **Within the county, every office is expected to utilize the centralized IT systems and services provided by the ADP Board**, and no parallel systems should be independently operated unless expressly authorized by the Board.

Sec. 5.0 – Policy and Procedure

1. **Acceptable Use of County IT Resources**
   Geauga County IT resources (including computers, networks, software, email, and Internet access) are provided to users for official County business purposes. All use of County IT assets must be **lawful, ethical, and in compliance with all applicable policies, licenses, and contracts**. Users are expected to exercise common sense and good judgment in their use of County technology. Limited personal use may be permitted for employees *during non-work time* (e.g. brief personal email or web browsing during breaks) if it does not interfere with work duties, does not consume significant resources, and is consistent with this policy and security requirements.
   Prohibited Activities: Users shall **not** use County IT resources for any activities that are unlawful, unethical, or contrary to County interests. Examples of prohibited use include, but are not limited to:
   - Engaging in any criminal conduct, such as unauthorized access (hacking), theft of information, or harassment/bullying using County systems.
   - Creating, accessing, downloading, or distributing material that is obscene, defamatory, discriminatory, harassing, or otherwise offensive (except as authorized for law enforcement or other official purposes).
   - Using County IT resources for personal commercial gain or outside business activities, political campaigning, or for personal use that is excessive or violates any County policies.
   - Knowingly introducing malware, viruses, or engaging in any activity that could harm the County's systems or data.
   - Attempting to circumvent or disable **security controls** (e.g. firewall, antivirus, web filters) installed on County systems. Users must not deliberately disrupt network communication or otherwise interfere with the normal operation of IT services.

All users have a responsibility to use County IT assets in a manner that maintains IT **security** and **performance**. Any use that violates this policy or threatens County IT operations may result in immediate restriction of access and disciplinary action (see Sec. 6.0).

2. **User Account Security**
   Each user is accountable for actions performed under their assigned accounts and credentials. **Credentials (passwords, security tokens, access cards, etc.) must be kept confidential and must not be shared** with or delegated to others. Users shall follow County password policies, which require strong, complex passwords and utilize multi-factor authentication (MFA) where required. Users must never use another person's login credentials or allow someone else to use theirs. If a user believes their account or password may have been compromised, they must **report it immediately and change their password** (see also Incident Reporting in item 9). Users shall also log off or lock their workstations or sessions when not in use to prevent unauthorized access. By adhering to these practices, users support CIS Control guidelines on access management and help protect County systems from unauthorized entry.

3. **Privileged Access and Administrative Responsibilities**
   IT professionals, system administrators, and any users with **elevated or administrative access** must adhere to the principle of least privilege and exercise additional care in their activities. Privileged accounts (such as domain administrators, network admins, or accounts with advanced system rights) **shall be used only for authorized administrative tasks** and not for general day-to-day use. Administrators should use a standard user account for routine work and log in with privileged credentials only when necessary. **All administrative access must be secured with multi-factor authentication** and strong passwords and must never be shared. Individuals with administrative privileges are expected to **avoid any abuse of privileges** – for example, accessing data or systems beyond the scope of their duties is strictly prohibited. Every action performed with elevated privileges should be traceable to an individual account, and such actions may be logged and audited by the ADP DATA or DARC Departments. Administrators must also ensure that any changes to system configurations are authorized and documented. Compliance with this policy by privileged users is critical, as it aligns with CIS Controls for controlling administrative privileges and helps prevent security incidents resulting from misuse of high-level access.

4. **Remote Access and Virtual Private Network (VPN) Usage**
   Remote access to County networks and systems (for example, through VPN, remote desktop, or web-based portals) is allowed **only via County-approved methods** and with explicit authorization. All remote connections must use secure, IT-department-approved solutions – typically the County's enterprise VPN or remote access gateway – which employ strong encryption and authentication. **Multi-factor authentication** is required for remote logins to enhance security (e.g. a one-time token or app in addition to a password). Users must not use unauthorized remote control software or services to connect to County systems. When connecting remotely, users are responsible for using a **trusted device and network**: remote sessions should ideally be initiated from County-

managed devices. If personal or non-County devices are used, they must meet security requirements (such as up-to-date antivirus, security patches, and possibly a security check by IT) and be approved for remote access. Users are expected to avoid using public or unsecure Wi-Fi networks for remote work.

User Responsibilities for Remote Sessions: Remote access users should ensure that they protect the confidentiality of any County information accessed remotely. This includes being mindful of who can view their screen (use privacy screens or avoid working with sensitive data in public areas) and not downloading or copying sensitive data to unmanaged devices. All sessions should be logged off or disconnected when finished or when unattended. Credentials used for remote access are subject to the same security standards as internal use and **must never be shared** or exposed. The County may monitor remote access sessions and activity; by using the VPN or remote systems, users consent to such monitoring. Any unauthorized use of remote access or violation of remote access rules may result in immediate revocation of remote access privileges and further enforcement action.

Contractors or third parties requiring remote access must do so via County-approved vendor access solutions, use only the credentials provided to them, and abide by this policy and any additional terms in their contracts.

5. **Use of Cloud Services and External Systems**

   Use of cloud computing services (such as software-as-a-service applications, cloud storage, or hosted platforms) for County business must be **authorized by the Department of IT**. Users shall **not store or transmit County data via personal or unapproved cloud services**. For example, employees and contractors are prohibited from uploading County files to personal cloud storage accounts (e.g. personal Dropbox, Google Drive) or using unauthorized collaboration tools to conduct County business. All cloud services used must have proper contracts or agreements in place that meet the County's security and compliance requirements (including applicable privacy laws and data protection standards). County data, especially sensitive or confidential information, should reside only in **approved environments** – such as the County's official Microsoft 365 cloud, other government community cloud services, or on-premise systems – and **must not be exported** to third-party systems without management approval and risk assessment.

   When using authorized cloud services, users must adhere to the same security policies that apply to internal systems. This includes using strong authentication, maintaining data confidentiality, and not granting access to cloud data to any unauthorized individuals. Any **vendor or third-party** providing cloud-based solutions to the County must comply with this policy and any applicable data handling agreements. The Department of IT will periodically review cloud services for compliance. **Note:** Public users who access County-provided web services or open data portals must also use such resources only for their intended public purposes and not attempt to compromise the County's cloud systems.

6. **Protection of Data and Confidential Information**

   All users have a duty to protect County information from unauthorized access, disclosure, alteration, or destruction. Users shall handle data in accordance with the County's data classification and privacy policies. **Sensitive or confidential information** (e.g. personal identifying information, law enforcement data, health records, financial data) must not be emailed to non-County addresses, uploaded to unapproved systems, or stored

on personally owned devices without explicit written authorization. When transmitting sensitive data to authorized external parties, approved secure methods (such as encrypted email or secure file transfer) must be used. Users must not divulge confidential data to anyone unless it is part of their official duties and the recipient is authorized to have the information.

Additionally, users should exercise caution when handling any County data: for instance, do not leave documents or screens containing sensitive information unattended in public view. All devices should be locked or logged out when not in use. **Portable storage** (like USB drives) should be used sparingly and must be encrypted if they contain sensitive data. Any loss or suspected compromise of sensitive information must be reported immediately (see Incident Reporting). By following these practices, users help the County comply with CIS data protection controls and other legal data security mandates.

Furthermore electronic records created or stored on County computers may constitute a public record which may be subject to disclosure under the Ohio Public Records Act, Ohio Sunshine Laws, and other State or Federal laws.

7. **System Security and Asset Use**

   Users are expected to treat all County IT equipment and systems with care and to follow ADP guidelines for secure configuration. **No user may install software or hardware** on County computers or the network without prior approval from ADP. This includes downloading unauthorized applications, utilizing personal hardware like routers or access points on the County network, or introducing any device that could pose a security risk. All software used must be properly licensed and approved; the use of pirated or unlicensed software on County systems is strictly forbidden. Users must not deliberately **alter system settings or configurations** in a way that undermines security (for example, disabling antivirus programs, firewall settings, or security logging). **Bypass of access controls** or attempting to elevate privileges without authorization is a serious violation.

   County-owned devices should only be used by authorized persons and primarily for work-related tasks. Users have the responsibility to promptly install (or allow IT to install) required security updates and patches on their assigned devices. If a device is found to be out of compliance (e.g. missing critical updates or security software), ADP may restrict its network access until the issue is resolved. In accordance with CIS best practices, the County maintains standard secure configurations for systems; users shall not deviate from these standards on their own. Any exception or special configuration must be approved by ADP and documented. Physical security of devices is also important – users should secure laptops or mobile devices when traveling or unattended, to prevent theft or unauthorized use.

8. **Monitoring and Auditing of IT Usage**

   All use of Geauga County IT resources is subject to monitoring and audit. Users should have **no expectation of privacy** in their use of County equipment, networks, and services. ADP and authorized officials may, at any time and without further notice, access, monitor, and/or review any information stored or transmitted on County systems. This includes email, internet usage, files stored on network drives, logs of system access, and any other records. Such monitoring will be conducted in compliance with applicable laws and is intended to support operational integrity, security reviews, and investigations of suspected misconduct. Use of County IT resources

constitutes consent to this monitoring and auditing.
ADP will also perform **regular audits** of accounts, user access rights, and system configurations to ensure compliance with this policy and other security standards. For example, periodic reviews of user privileges may be conducted (aligned with CIS Controls for access control management) to verify that each user's access is appropriate for their role. Network and system logs may be analyzed to detect unauthorized activities or policy violations. Users and departments are expected to cooperate fully with any auditing or monitoring processes. Findings from audits may be reported to management and could result in remedial actions or policy adjustments to improve security.

9. **Incident and Violation Reporting**
   All users must promptly **report any security incidents, potential data breaches, or policy violations** to the appropriate authorities. Security incidents include, for instance, evidence of malware infection on a computer, the loss or theft of a device that contains County data, accidental disclosure of sensitive information, or any situation where an unauthorized person may have accessed County systems or information. Users should also report if they observe another individual violating this Acceptable Use Policy or other IT security policies. Reports should be made to DARC or the supervisor/management in charge, following any established incident reporting procedures. The County will investigate reported incidents and take appropriate actions to mitigate risks and address any violations. Prompt reporting is essential to minimize damage and ensure the County can fulfill any legal or contractual breach notification obligations. **Whistleblower Protection:** Users who report security issues or policy violations in good faith will not face retaliation for doing so; however, false reports made maliciously will be subject to disciplinary action.

Sec. 6.0 – Policy Compliance

All covered users (employees, IT personnel, contractors, etc.) are required to **acknowledge and sign** this Acceptable Use Policy, indicating that they have read, understand, and agree to abide by it. New employees and third-party users must sign the policy prior to receiving access to County IT systems, and **annual refresher acknowledgment** may be required thereafter. ADP may also require users to complete periodic security awareness training related to this policy.

Failure to observe and adhere to this policy may result in disciplinary action, up to and including **revocation of access credentials, termination of employment or contract**, as well as possible civil and criminal penalties. Violations by County employees will be addressed in accordance with County HR policies and any applicable union or civil service rules. Contractors or vendors found in violation may face termination of their contracts and removal from County networks. Members of the public who violate these terms (for example, by abusing public-facing systems or engaging in attacks) may be denied further access and could face legal consequences under the law. The County may temporarily suspend a user's access to IT resources if a violation is suspected, pending an investigation. **Users are responsible for compliance** with this policy and other related policies; lack of knowledge of the policy will not be considered a defense for violations. The County reserves the right to hold users financially liable for damages or costs incurred due to intentional policy violations or negligence.

Sec. 7.0 – Policy Revisions

This policy will be reviewed at least annually or as needed to reflect new threats, technologies, or compliance requirements. Updates will be documented and communicated accordingly.

Below is the revision history for this policy:

Signed by:
5EGDE9230E05438...

7/17/2025 | 08:13:34 EDT

Charles E. Walder, Geauga County Auditor
Automatic Data Processing Board Chief Administrator

Date