Automatic Data Processing Board

Geauga County Cybersecurity Program (O.R.C. § 9.64 Compliance Policy)

September 9, 2025

Executive Summary

Geauga County is implementing a comprehensive Cybersecurity Program to safeguard the County's data, technology systems, and critical services against cyber threats. This program is established in direct response to Ohio Revised Code § 9.64, which mandates that every local government adopt formal cybersecurity policies consistent with industry's best practices. The program outlined in this document serves to ensure the confidentiality, integrity, and availability of County information assets while maintaining public trust in our digital infrastructure. Key components of the program include proactive risk identification and management, robust threat detection and incident response procedures, business continuity and recovery planning, and ongoing cybersecurity training for all County employees. By aligning with the Center for Internet Security (CIS) Controls, Geauga County's Cybersecurity Program will not only meet state legal requirements but also significantly strengthen our defense against ransomware, data breaches, and other cyber incidents.

Purpose and Benefits: This Cybersecurity Program is designed to protect Geauga County's operations and constituents from the escalating risks of cyberattacks. It provides a structured approach to identify vulnerabilities, prevent incidents where possible, and respond effectively when incidents occur. The program's benefits include protecting sensitive resident and financial data, minimizing downtime of critical public services, and reducing the financial and reputational damage that can result from cyber incidents. By formally adopting this program, the County demonstrates due diligence in cyber risk management, complies with state law, and leverages best practices to improve its security posture. In addition, the program integrates existing ADP security policies (on acceptable use, password/multi-factor authentication, etc.) into a unified framework, ensuring consistency and clarity for all users. The end result is a resilient cybersecurity environment that helps maintain continuity of government services and safeguards public resources for the benefit of all Geauga County residents.

Position Statement – Necessity of the Cybersecurity Program

Geauga County is committed to protecting public data and infrastructure from cyber threats, and this Cybersecurity Program is both a legal mandate and a critical investment in our County's future. Recent years have seen a sharp increase in cyberattacks on government entities of all sizes. Even in our region, several Geauga County townships experienced breaches and ransomware attacks in 2024–2025, underscoring that no community is immune. County Auditor Charles Walder has emphasized that it's not a question of *if* an attack will occur, but *when*, stating that "preparedness is what it's all about". As the steward of taxpayer funds, sensitive citizen information, and critical services (from law enforcement networks to water systems), Geauga County has an obligation to anticipate these threats and defend against them.

Ohio's new law (House Bill 96, codified as O.R.C. § 9.64) makes this obligation explicit by requiring every county to adopt a cybersecurity program and by prohibiting ransom payments without public approval. This legislation was enacted because cybersecurity is now fundamental to good governance and public safety. A major cyber incident could halt County operations, compromise personal data, and erode public trust. Geauga County's Board of Commissioners and Automatic Data Processing (ADP) Board recognize that strong cybersecurity is essential to fulfilling our duty to the public. By formally adopting this program, the County's leadership affirms a strong security posture and compliance with state law, while sending a clear message: Geauga County will proactively safeguard its digital assets and will not reward cybercriminals.

In summary, this Cybersecurity Program is necessary to (1) comply with legal mandates (avoiding penalties and ensuring eligibility for state cyber support), (2) address the escalating threat landscape (protecting against financial fraud, ransomware, and data theft), and (3) uphold the County's responsibility to protect public resources and services. Adopting this program will empower Geauga County to respond swiftly to incidents, minimize damage, and maintain continuity of operations in the face of cyber adversity. It is a prudent and required step to protect our community in the digital age.

Scope and Authority

This Cybersecurity Program applies to all Offices, agencies, and personnel of Geauga County in accordance with Ohio Revised Code § 307.847. It extends to County employees and officials, IT staff with elevated privileges, third-party contractors or vendors with access to County systems, and any local political subdivisions under the County's IT coordination (per O.R.C. § 307.847) that utilize ADP Board services. In practical terms, every County office and any township or municipal entity within Geauga County that is part of the County's network or IT services is covered under this program. All such entities and users must adhere to the cybersecurity policies and procedures herein when accessing or using County-managed data, systems, and networks.

Legislative Authority: Ohio Revised Code § 9.64(C) requires the County's *legislative authority* to formally adopt a cybersecurity program. For Geauga County, the Board of County Commissioners – in coordination with the Automatic Data Processing (ADP) Board – serves as the legislative authority enacting this program as official County policy. This program is issued under the authority of the Board of Commissioners and is administered by the Geauga County ADP Board and its departments, pursuant to Ohio law (O.R.C. § 307.84 and 307.847) which empowers the ADP Board to oversee county-wide IT governance and security. The County Auditor (as Chief Administrator of the ADP Board) is charged with enforcing cybersecurity standards across all covered entities. By Commissioner resolution, this Cybersecurity Program is adopted as County policy effective immediately and supersedes any conflicting local directives. All County agencies and partnering subdivisions are required to cooperate with ADP in implementing these security measures.

Alignment with Best Practices: In accordance with O.R.C. § 9.64(C), Geauga County's Cybersecurity Program is consistent with generally accepted cybersecurity best practices, drawing on the Center for Internet Security (CIS) Controls. Geauga's approach follows the core functions of Identify, Protect, Detect, Respond, and Recover, ensuring a defense-in-depth strategy. Our primary internal policy (Geauga County Cybersecurity Policy ADP-25-F-003) is already aligned with the CIS Critical Security Controls, covering areas such as asset management, access control, network security, incident response, and more. This program leverages that foundation and maps each requirement of the Ohio law to our existing controls and new initiatives. By adhering to industry-standard frameworks, Geauga County ensures that its cybersecurity efforts meet a high standard of rigor and are continuously informed by current threat intelligence and proven practices. This alignment also facilitates external audits and assessments, as it mirrors the criteria used by oversight bodies like the Auditor of State and cybersecurity insurance providers. The sections below detail the components of the program, each corresponding to a specific requirement of O.R.C. § 9.64 and the CIS framework categories.

Integration with Existing County Policies

Geauga County's Cybersecurity Program builds upon and integrates several pre-existing County IT policies. Rather than duplicating those documents, this program references them as integral components of our overall security framework **(all remain in full effect)**:

- **Geauga County Cybersecurity Policy (ADP-25-F-003):** A comprehensive technical policy aligned with CIS Controls that establishes baseline security controls (asset inventory, secure configuration, access management, patch management, logging/monitoring, incident response planning, etc.) for all County IT systems. ADP-25-F-003 is incorporated by reference into this program – it details many of the "Protect" controls that reduce risk on a daily basis. All County departments must continue to follow ADP-25-F-003's standards (e.g. maintaining inventories, hardening systems, enforcing least privilege access, etc.) as a core part of the Cybersecurity Program.

- **Acceptable Use Policy (ADP-25-A-004):** Defines acceptable and secure use of County IT resources by employees, officials, and other users. It covers user responsibilities, prohibited activities, and general security practices (such as not sharing credentials, avoiding unsafe websites, proper use of email). By following ADP-25-A-004, users help protect the County from threats caused by human error or misuse (such as phishing and malware infections). This Cybersecurity Program reinforces that all personnel must abide by the Acceptable Use rules as a first line of defense.

- **Multi-Factor Authentication & Password Policy (Policy #28-22-018):** Mandates strong authentication controls for County systems, including the use of multi-factor authentication (MFA) for all user logins and robust password requirements. Per this policy, all County network and email accounts *must* use MFA and comply with strict password complexity and length rules (e.g. a minimum of 25 characters, with mixes of character types). This is critical to preventing unauthorized access. The Cybersecurity Program adopts these authentication standards to ensure that only authorized individuals can access sensitive systems and data.

- **Incident Reporting and Response Policy (ADP-25-F-005):** Establishes procedures for reporting and escalating cybersecurity incidents within the County and to external authorities. It defines what constitutes a reportable incident and outlines the immediate steps for County personnel to take (such as contacting the ADP Department of Advanced Research and Cybersecurity (DARC) team). ADP-25-F-005 also aligns with the state's notification requirements, ensuring the County meets the 7-day and 30-day reporting rules in O.R.C. § 9.64(D). This Cybersecurity Program incorporates that policy by reference to handle incident communications; all staff must follow its reporting procedures in the event of a suspected cyber incident.

- **Geauga County Cybersecurity Awareness Training Policy (ADP-25-F-006):** Establishes requirements and expectations for all Geauga County Network users to complete cybersecurity awareness training including the yearly Ohio Persistent Cyber Improvement (OPCI) training provided by The Ohio Cyber Range Institute (OCRI) and funded by the State of Ohio and Cybersecurity and Infrastructure Security Agency (CISA), as well as additional training provided throughout the year by ADP. Additionally, it specifies training requirements based on roles and responsibilities in the organization, monthly simulated phishing campaigns, and remedial action and procedures for non-compliance.

By integrating these existing policies, Geauga County ensures its Cybersecurity Program is comprehensive and coherent. Each policy addresses specific aspects of cybersecurity (from user behavior to technical controls to incident handling), and together they fulfill the requirements of state law. Employees and officials should view this program and the above policies as part of one unified governance structure on cybersecurity. Compliance with all of them is mandatory. References to specific policies will be made in the sections below, to show how they support each facet of the program.

Risk Assessment and Critical Function Identification

Identify Critical Assets & Risks: Geauga County has identified and prioritized its critical functions, systems, and information assets, and assessed the cybersecurity risks associated with each. In practice, DATA maintains up-to-date inventories of all hardware and software in use (as required by ADP-25-F-003) and determines which of those systems are essential to government operations or hold sensitive data. Critical assets likely include financial systems, law enforcement and 911 dispatch systems, water and utility control systems, election infrastructure, email and communication platforms, and any databases containing personally identifiable information of citizens. For each critical system, the County's IT security team, DARC, will evaluate potential threats and vulnerabilities – for example, risks of data breach, service disruption, ransomware, etc.

Risk Assessment Process: The County will conduct periodic risk assessments to gauge the potential impact of various cyber threats on critical operations. This involves analyzing how a breach or outage of a given system would affect public services, safety, finances, and the County's legal or reputational standing. For instance, the team will assess scenarios such as loss of 911 dispatch capability, tampering with financial/payroll data, exposure of citizen personal records, or prolonged email system failure. The potential impacts of a cybersecurity breach are identified and documented for each scenario, as required by law. These impacts range from minor inconveniences to major service failures or public safety hazards. By understanding worst-case outcomes (e.g. inability to deliver emergency services, or theft of thousands of identities), the County can prioritize security measures to prevent those outcomes. High-risk systems or processes will receive enhanced protection and more frequent monitoring.

Mitigation of Identified Risks: Once risks are identified, ADP will address them through appropriate controls and remediation steps. This might include strengthening network protections around critical systems, ensuring redundant systems or backups are in place for essential services, and applying software patches or upgrades to eliminate known vulnerabilities. Any high-risk findings from vulnerability scans or audits will be escalated for prompt mitigation. The DARC department maintains a risk register or log and regularly reviews it with County leadership. Our goal is to reduce the likelihood and impact of security incidents by being proactive – patching weaknesses before they are exploited and implementing safeguards for mission-critical operations. Ultimately, this satisfies O.R.C. § 9.64(C)(1) and (C)(2) by providing a structured way to identify what needs protection and what the consequences would be if protections fail.

Supporting CIS Controls: This risk identification effort aligns with CIS Control #1 (Inventory and Control of Hardware Assets) and #2 (Inventory and Control of Software Assets), as well as CIS Control #3 (Data Protection). By knowing "what we have" and "what could go wrong," the County addresses the Identify function of CIS Controls. The ADP Board will be kept informed of major risk assessment results and will support necessary risk reduction measures (e.g. funding security upgrades or adjusting processes) as part of governance oversight.

Threat Detection and Monitoring

Continuous Threat Monitoring: ADP has implemented mechanisms to detect potential cyber threats and events across our networks and systems, satisfying O.R.C. § 9.64(C)(3). This includes deploying technical tools and processes to actively monitor for suspicious activity. Key elements of our detection capability are:

- **Network and Endpoint Monitoring:** Use of intrusion detection/prevention systems (IDS/IPS) at the network perimeter, and security agents on endpoints (servers, workstations) to flag malicious behavior. All County computers have anti-malware software and advanced endpoint protection that alerts IT staff if malware is detected or if unusual processes are running. Network firewalls and routers log inbound and outbound traffic, and those logs are aggregated for analysis. The ADP DARC team and/or a Security Operations Center service will continuously review alerts for signs of attacks (e.g. repeated failed login attempts, data exfiltration traffic, malware signatures).
- **Security Information and Event Management (SIEM):** The County either maintains a SIEM system or equivalent log management solution to correlate events from various sources (firewalls, servers, applications) in real time. This helps detect patterns that single devices might not catch – for example, a user account logging in from an unusual location combined with a spike in data access. Automated rules generate alerts that are sent to the DARC incident response team for investigation.
- **Threat Intelligence Integration:** The County will leverage threat intelligence feeds, including information from the Ohio Cyber Integration Center (OCIC) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), to stay updated on emerging threats targeting local governments. If OCIC or MS-ISAC issues alerts about specific malware or phishing campaigns, our monitoring tools can be tuned to watch for those indicators.
- **Email and Web Security Filtering:** Since email is a primary entry point for cyberattacks, the County uses email security gateways and filters to block spam, phishing attempts, and known malicious attachments or links. Similarly, web filtering is in place to prevent users from visiting known malicious websites (blocking drive-by downloads or fake login pages). These tools generate alerts when they block a threat, allowing IT to follow up with the user or system affected.

Together, these detection mechanisms ensure that if a potential cybersecurity event occurs, it will be noticed as quickly as possible. Simply put, we are setting up an early warning system for cyber threats. This proactive monitoring is in line with CIS Controls (e.g. Control #8: Audit Log Management, Control #13: Network Monitoring and Defense) and best practices recommended by CIS and NIST. By having "eyes on glass" and automated alerts 24/7, Geauga County can detect anomalies or intrusions in their early stages, which is crucial for prompt response.

Threat Detection Procedures: When a threat or incident indicator is detected, clear procedures are in place for analysis and escalation (per our Incident Response Policy). The ADP DARC team will investigate the alert to confirm if it represents a true incident (as opposed to a false alarm). This may involve checking system logs, running malware scans, or observing network traffic. If a cybersecurity incident is suspected, the DARC team will immediately initiate the incident response process (detailed in the next section). The County's goal is to avoid "silent failures" – every significant alert will be

reviewed, and if malicious activity is confirmed, it will trigger our containment and notification protocols without delay. This fulfills the O.R.C. requirement to have mechanisms to detect potential threats and events, ensuring we aren't caught unaware by attacks.

Incident Response and Containment Procedures

Despite our best preventive measures, incidents may still occur; when they do, Geauga County will react swiftly and systematically. The Cybersecurity Program includes formal incident response procedures that establish communication channels, analysis steps, and actions to contain and eradicate cybersecurity incidents. These procedures are documented in the County's Incident Response Plan (IR Plan) and the Reporting/Escalation Policy ADP-25-F-005, which are aligned with CIS Control 17 (Incident Response Management). Key aspects of our incident response are as follows:

- **Immediate Reporting and Escalation:** Any County employee or IT staff who discovers or suspects a cybersecurity incident (e.g. malware outbreak, system breach, data loss, ransomware attack) must immediately report it to ADP DARC or the IT Service Desk. Front-line staff are instructed: "if you see something, say something" without delay. Early reporting is critical; there will be no penalty for false alarms, but failing to report an actual incident could greatly worsen its impact. Once the DARC incident response team receives a report, they log the incident and begin a preliminary investigation.

- **Activation of Incident Response Team:** The County's incident response team (DARC, including cybersecurity specialists and system administrators) will be activated immediately upon confirmation that an incident is occurring. This team has defined roles: e.g., a lead incident handler, a communications liaison, and technical specialists for affected systems. The team follows a structured Incident Response Plan that aligns with CIS Control guidelines. We ensure that all team members are trained, and drills are conducted routinely so that everyone knows their role when an event happens.

- **Communication Channels and Leadership Involvement:** Upon activation, the incident team establishes clear communication channels. Internally, the incident lead will promptly escalate to County leadership. The Deputy Chief Administrator of ADP and the Chief Administrator (County Auditor) are to be notified as soon as a serious incident is verified. The County's executive leadership (ADP Board and Commissioners as appropriate) will be informed in the early stages of any major breach or ransomware event. Regular updates will be provided as the incident unfolds. If multiple County offices are affected, a coordinated communication (e.g. conference call or emergency meeting) will ensure all stakeholders remain informed. The IR Plan also includes communication templates for notifying employees if they must take actions (like disconnecting from the network or not opening email), and for public information officers if any public communication becomes necessary. Under O.R.C. § 9.64(C)(4), establishing these communication procedures is critical to managing incidents effectively. No one will be left guessing about who should be called or what information can be shared – it's pre-defined.

- **Containment Actions:** The top priority in any confirmed cybersecurity incident is containing the threat to prevent further damage. Depending on the situation, this may include isolating affected computers (taking them off the

network), shutting down specific services, revoking compromised user accounts or changing passwords, and blocking malicious IP addresses or domains at the firewall. For example, if a ransomware infection is spreading, the team will rapidly disconnect infected machines and potentially shut down portions of the network to halt propagation. If a server is breached, it may be taken offline or segmented. These actions are taken immediately, even as analysis continues. Containment decisions will be made by the incident lead in consultation with ADP personnel, prioritizing the safety of data and continuity of critical operations. We recognize that containment can sometimes disrupt services (e.g., shutting off a server), but it is necessary to stop the bleeding. Our policies authorize the ADP Chief Administrator or designee to take emergency actions to protect the County's systems, even if it means temporary inconvenience.

- **Eradication and Recovery:** Once the threat is contained, the incident team moves to eradicate the cause of the incident (e.g. removing malware, closing vulnerability, expelling intruders from the system) and then to recover operations. Eradication may involve steps like wiping and re-imaging infected devices, applying security patches, or restoring systems from clean backups. (Recovery is discussed in more detail in the next section.) Throughout this process, the incident must be carefully analyzed and documented. The team will preserve forensic evidence where appropriate – for instance, malware samples or logs – especially if law enforcement might be involved. Analysis will seek to answer how did this happen, what data or systems were affected, and what corrective measures are needed.

- **Internal Reporting and Documentation:** ADP's DARC team will maintain an incident log and report for every incident. This includes a timeline of all actions taken, systems affected, communications made, and results of investigations. Proper documentation is not only a best practice (for learning and accountability) but also required for eventual state reporting. By keeping detailed records, we can later review our response for any improvements and have evidence of compliance with reporting laws. Notably, all such incident records are kept confidential and are exempt from public records disclosure (see the section on Confidentiality below).

These incident response and containment protocols ensure that Geauga County can swiftly mitigate any cybersecurity incident and minimize harm. Whether it's a virus outbreak, network intrusion, or ransomware encryption, everyone from end-users to IT experts knows the plan: report immediately, get the right people involved, communicate clearly, contain the damage, and restore services. The County's approach reflects best practices and complies with O.R.C. § 9.64(C)(4) by defining how we "establish communication channels, analyze incidents, and take actions to contain" any cybersecurity incident. By being prepared and practiced, we aim to handle incidents in a calm, efficient, and law-abiding manner.

Recovery and Restoration of Services

After containment and eradication of a cybersecurity incident, Geauga County will focus on restoring affected systems and repairing any damage to our infrastructure. The Cybersecurity Program establishes procedures for recovery and post-incident security improvements in line with O.R.C. § 9.64(C)(5). Recovery procedures include:

- **Data Backup and Restoration:** The County maintains regular data backups for all critical systems (as dictated by our backup policy in ADP-25-F-003). In the event that data or systems are corrupted, encrypted (by ransomware), or otherwise rendered unavailable, IT staff will restore from the most recent clean backups. Multiple backup layers are used: on-site backups for quick recovery and off-site or cloud backups for disaster recovery (in case our facilities are compromised). We routinely test backups to ensure their integrity. If an incident occurs, priority is given to restoring essential services first (for example, financial systems needed for payroll, or law enforcement databases needed for public safety). The recovery team will follow established Disaster Recovery Plans (DRPs) which detail the order of restoration and key contacts for each major system. Using backups, we aim to avoid paying ransoms and minimize downtime – a strategy strongly reinforced by the state's stance against ransom payments.

- **Infrastructure Repair and System Hardening:** For any hardware or software components damaged or exploited during the incident, the County will repair or rebuild them in a secure manner. This may involve re-imaging computers, reinstalling clean operating systems, replacing compromised equipment, or applying urgent patches. As systems are brought back online, we will ensure that all security updates are applied, and any backdoors or malware are removed. The recovery phase is also an opportunity to harden our defenses to prevent a recurrence. For example, if an incident revealed a gap (such as an open firewall port or an outdated application), those issues will be fixed before that system is returned to production. Recovery procedures thus dovetail with longer-term remediation: we do not simply restore the status quo but rather improve the security posture where possible. This addresses the O.R.C. requirement to not only repair the infrastructure but also maintain security after the incident.

- **Validation and Testing:** Before declaring the incident fully resolved, the IT team will validate that affected systems are operating normally and securely. This might include running additional virus scans, verifying data integrity (no unauthorized alterations), and monitoring system behavior closely for a period of time. Users may be asked to confirm that their applications are working correctly. In a severe incident, we might also bring in third-party experts or perform a security audit to ensure that all traces of the attack have been eradicated. Only after thorough validation will the incident be closed and systems returned to routine operation.

- **Post-Incident Analysis and Lessons Learned:** A critical part of recovery is holding a post-incident review to analyze what happened and how our response fared. The incident response team, along with relevant department leaders, will convene once things are stabilized to review the incident report: What was the root cause? Were there warning signs missed? What defenses failed or worked well? How did our team perform in detection and containment? From this analysis, we will derive lessons learned and identify any needed changes to policies, procedures, or configurations. For instance, a lesson could be that staff need additional training on recognizing phishing, or that a new tool is required for better monitoring. These lessons will be documented and presented to the ADP Board and County leadership. The Cybersecurity Program will be updated as necessary to incorporate improvements. Continuous improvement is a key principle of CIS frameworks – we treat every incident as a learning opportunity to strengthen our cyber defenses.

- **Continuity of Operations:** It's important to note that throughout an incident and recovery, the County will execute its Continuity of Operations Plan (COOP) to keep critical services running, even if at reduced capacity or via workarounds. For example, if our primary network is down, essential functions may revert to manual processes or alternate communication methods temporarily. The Cybersecurity Program coordinates with broader emergency management plans to ensure that the public experiences minimal disruption. Recovery procedures are designed to reduce downtime and prioritize essential functions, as recommended in the O.R.C. and best practices. Our aim is that even during a cyber crisis, Geauga County government can continue to serve its citizens.

By establishing and practicing these recovery steps ahead of time, Geauga County will be prepared to bounce back quickly from cyber incidents. O.R.C. § 9.64(C)(5) explicitly requires having procedures for infrastructure repair and security maintenance post-incident, and this program meets that mandate through comprehensive backup, restoration, and improvement processes. These efforts also align with CIS Controls (such as Control #11: Data Recovery Capabilities and Control #10: Malware Defenses, ensuring clean restoration). Ultimately, a prompt and secure recovery not only restores public services faster but also reinforces public confidence in the County's resilience.

Security Awareness and Training

Technology alone cannot secure the County; our workforce is the first line of defense. Therefore, the Cybersecurity Program mandates regular security awareness training for all Geauga County employees and officials, fulfilling O.R.C. § 9.64(C)(6). The County will establish a robust training and awareness program with the following elements:

- **Annual Mandatory Training:** Every County employee (and any contractors with network access) must complete cybersecurity training at least once per year. This training will cover fundamental topics such as recognizing phishing emails, safe internet usage, proper data handling, creating strong passwords, and how to report suspected security incidents. The training content is updated each year to address evolving threats (for example, recent social engineering scams or ransomware trends). Completion of the annual training is tracked and recorded – non-compliance may result in corrective action or loss of system access until training is done, underscoring its importance. Notably, the State of Ohio provides free annual cybersecurity training resources (e.g. through the Ohio Persistent Cyber Improvement (O-PCI) program), and the County utilizes these whenever possible. State-provided training satisfies the legal requirement and ensures consistency with statewide best practices. By using these resources, we also save costs and benefit from materials tailored for local government users.

- **Role-Based and Ongoing Training:** In addition to the basic annual module for all staff, the County will implement role-based training for users in specialized positions. For example, IT administrators will receive deeper technical training on topics like secure server configuration, incident response procedures, and advanced threat detection (since they play key roles in those areas). Department heads and managers may get training on cybersecurity governance and risk management relevant to their oversight duties. Employees who handle sensitive data (e.g. in Finance or HR) might receive extra instruction on data protection regulations. The County will also conduct periodic phishing email simulations and security reminders throughout the year to keep awareness high. If users fall for a

simulated phishing test, they may be assigned refresher training to reinforce learning. The goal is a culture of continual vigilance, not a one-and-done approach.

- **New Hire Orientation:** Cybersecurity expectations will be introduced as part of onboarding any new employee or official. New hires must complete an initial security training module within their first days/weeks of employment. This ensures they understand the County's policies (like Acceptable Use and MFA requirements) and know how to spot common threats from the start. They will also be briefed on the importance of their role in protecting County data, no matter their job title.
- **Executive and Elected Officials Awareness:** The program also calls for periodic briefings or workshops for the County's leadership (e.g. Commissioners, elected officials, directors). High-level decision-makers need awareness of cyber risks and their responsibilities in supporting cybersecurity (for instance, understanding why certain budget expenditures or emergency actions are needed). These sessions will cover threat trends, the County's cyber readiness status, and tabletop exercises for incident response decision-making, including the scenario of a ransomware attack where a payment decision might come to the Board. Ensuring top-level buy-in and understanding is key to a successful cybersecurity posture.

Training efforts will be coordinated by ADP, possibly in partnership with HR for tracking completions. All training records will be kept (securely) as evidence of compliance with the annual training mandate. Under O.R.C. § 9.64, the frequency, duration, and content of training should correspond to each employee's duties – our program accomplishes this by providing baseline annual training for everyone and additional targeted training for those with greater security responsibilities. This comprehensive training program maps to CIS Control 14: Security Awareness and Skills Training, which is proven to reduce the likelihood of human error leading to incidents. Educated employees are far less likely to fall for scams or make costly mistakes, and they become an active part of our defense by reporting suspicious activities.

By cultivating a cyber-aware workforce, Geauga County not only complies with the law but also significantly enhances its overall security. Users will be reminded that cybersecurity is part of everyone's job. The training initiative ultimately seeks to foster a culture of security within the County – one where good habits are second nature and people understand that their vigilance protects the community's interests.

Incident Reporting Obligations (External Notifications)

In addition to internal handling of incidents, Geauga County is legally required to report certain cybersecurity incidents to state authorities. O.R.C. § 9.64(D) establishes two tiers of external notification whenever a significant cybersecurity or ransomware incident occurs. The County's policy is to fully comply with these mandates, using the procedures outlined in ADP-25-F-005 to ensure timely reporting. The requirements and our implementation are as follows:

- **7-Day Notification to Ohio Homeland Security:** Following the discovery of a cybersecurity incident or ransomware incident, the County (through its legislative authority or a designee) must notify the Executive Director

of the Ohio Division of Homeland Security within 7 days. In practice, Geauga County will report the incident to the Ohio Cyber Integration Center (OCIC), which is operated by Homeland Security, as they are the likely designated recipient of such reports. The "clock" for this seven-day window starts as soon as the County discovers the incident (even if the incident is still ongoing or under investigation). Our incident response plan dictates that, as soon as the incident is confirmed and contained enough to gather basic details, the ADP Chief Administrator (County Auditor) or their designee will prepare the 7-day report. The content of the report will include a summary of what happened, which systems or data were affected, when it was detected, and what immediate actions were taken. We will use the reporting format or online portal prescribed by the Ohio Homeland Security Executive Director to submit this information. The ADP DARC team will assist with the technical details, but an authorized County executive (as required by the state) will formally submit the notification. Geauga County's goal is to make this notification as soon as possible, not waiting until the 7th day if information is available sooner. Early reporting can prompt state assistance or guidance that may help our response.

- **30-Day Notification to Ohio Auditor of State:** Additionally, the County must notify the Auditor of State's office within 30 days of discovering the incident. This will typically take the form of a more detailed incident report, since by 30 days a fuller investigation can be completed. The Auditor of State may have a specific form or an incident reporting system (the law allows them to prescribe the manner of reporting). Geauga County will comply by submitting the required information, which is expected to cover the nature of the incident, its impact, the steps taken to resolve it, and any ongoing remediation or improvements. The ADP DARC department will compile this report and coordinate with the County Auditor (as Chief Administrator) to ensure it is submitted on time. Again, we will strive to file this report well *before* the 30-day deadline if possible, providing updates to the Auditor's office as new information emerges. Timely reporting to the Auditor of State is not only a legal duty but also beneficial – it allows the Auditor to offer any support or include the incident in their oversight processes, and it demonstrates the County's transparency and diligence in handling the matter.

These notifications will be made for any incident that meets the threshold of a "cybersecurity incident" or "ransomware incident" as defined in the law (essentially, significant events impacting confidentiality, integrity, or availability, not minor routine malware). If there is uncertainty about whether an incident qualifies, the County will err on the side of reporting to ensure compliance. The ADP Board's policy is clear that *the responsibility to report lies with the County's legislative authority (ADP Board and Commissioners)*, and ADP will facilitate and verify the process. Internally, ADP will maintain up-to-date contact information and any required forms for state reporting (aligned with CIS Control 17.2: having information ready for external reporting). The incident documentation prepared during response will greatly aid in assembling these reports, ensuring consistency and accuracy of information.

By adhering to these 7-day and 30-day reporting rules, Geauga County not only stays compliant with O.R.C. § 9.64(D) but also contributes to a stronger statewide cybersecurity posture. These reports feed into state efforts to analyze threat patterns and can unlock additional resources for the County (for example, the OCIC might send incident response support if needed). The County views state notification not as merely a requirement, but as an opportunity to engage with partners in Homeland Security and the State Auditor's office for guidance and improvement. Our Incident Response Policy (ADP-25-F-005)

explicitly includes these notification steps, so that during the chaos of incident response, the legal reporting deadlines are not overlooked.

Finally, we note that beyond these required reports, we will also consider voluntary notifications to other entities as appropriate: for example, alerting the MS-ISAC or local law enforcement (FBI cyber task force) especially in cases of criminal ransomware or data theft. Such actions do *not* replace the state-mandated reports but supplement them. All external communications will be handled with confidentiality and integrity, ensuring accurate information is provided. By formalizing these reporting obligations in our program, Geauga County demonstrates transparency and accountability in its cybersecurity governance.

Ransomware Incident Policy and Prohibition on Payments

Ransomware is one of the most significant threats facing governments today. In a ransomware attack, critical files or systems are encrypted or rendered unusable by an attacker, who then demands a ransom (often money or cryptocurrency) for restoration of access. Geauga County's policy on ransomware is unequivocal: we will not pay ransoms to cyber criminals except under the extremely narrow conditions allowed by law, and even then only as a last resort. This stance is in line with O.R.C. § 9.64, which introduced a prohibition on local governments paying ransoms without prior legislative approval.

No Ransom Payments Without Commissioner Approval: O.R.C. § 9.64(B) explicitly states that if the County experiences a "ransomware incident," we are not permitted to pay or comply with the ransom demand unless the County's legislative authority (Board of County Commissioners) votes to approve the payment via a resolution or ordinance declaring it to be in the County's best interest. This is now the law in Ohio, and our County policy fully reflects this prohibition. By default, County administration and IT are forbidden from authorizing or facilitating any ransomware payment. If a ransomware attack occurs and County data is held hostage, the standing instruction is to focus on containment and recovery (e.g. restoring from backups) rather than considering payment. Only if recovery efforts fail and the consequences of not paying are truly dire would the County even contemplate paying; and in that scenario, the Board of Commissioners would have to be convened in an emergency session to debate and pass a resolution justifying the payment. This ensures a public, transparent decision with oversight, rather than a panicked private payout.

Geauga County's incident response plan has been updated to include this ransomware payment approval process. In practical terms, if ransomware hits: the Incident Response Team (DARC) will immediately assess the impact (What systems are affected? Do we have intact backups? Is critical public safety at risk?). The team will inform the County Auditor/ADP Chief Administrator and Commissioners of the situation as it develops. The default approach is to not pay and to instead use backups and other means to restore systems. Paying ransom is strongly discouraged by law enforcement and security experts, because it funds criminal activity and offers no guarantee of data return. Geauga County aligns with this best practice. We have invested in backups and redundant systems precisely so that we do not need to rely on a criminal's decryption key.

However, in an extreme case where human life, health, or truly critical operations hang in the balance (for example, a ransomware attack crippling 911 dispatch or a hospital system, where backup restoration has failed), County leadership might consider the ransom as a last resort. The O.R.C. 9.64(B) process would then be invoked: the Board of Commissioners would hold an emergency meeting (likely executive session followed by a public vote) to either approve or reject the ransom

payment. Any approval must state why paying is in the County's best interest (for instance, if lives are at stake or costs of not recovering data exceed the ransom in an overwhelming way). This decision and reasoning would become part of the public record via the resolution. If no resolution is passed, no County official may move forward with payment – doing so would violate the law. If a resolution does approve payment, the County will coordinate with law enforcement before and after paying, and will document all steps (the payment, the outcome, etc.) in the incident report.

Ransomware Prevention and Preparation: Recognizing the severity of ransomware threats, our Cybersecurity Program places heavy emphasis on prevention and preparatory measures so that paying a ransom never becomes a necessity. This includes maintaining offline backups of all critical data (so we can restore without decryption keys), network segmentation (so that ransomware spreading in one department can be isolated), up-to-date anti-malware on all systems, and regular training to avoid the phishing emails or unsafe downloads that often lead to ransomware infections. The County also keeps an incident playbook specifically for ransomware scenarios, which outlines the technical steps to take (e.g. isolate infected machines, secure backup copies, communicate with law enforcement, etc.) and the managerial steps (legal consultation, Commission notification). This playbook enshrines the no-payment principle clearly, stating that ransom payment is a last resort option requiring Board approval.

Geauga County's strong anti-ransomware stance is intended to do two things: discourage attackers (knowing we are unlikely to pay and have protection in place) and assure the public that we will not expend their tax dollars to reward criminal extortion unless absolutely unavoidable. This stance is fully supported by O.R.C. § 9.64(B)'s spirit of deterring ransom payments and encouraging investment in alternative recovery methods. Additionally, by requiring public justification for any payment, it aligns with our values of transparency and fiscal responsibility. In summary, if hit by ransomware, Geauga County will first and foremost rely on its backups and response plans rather than giving in to attacker demands. Only under a Commissioner-approved resolution, with clear justification, would that position change – and even then, such a decision would involve consultation with law enforcement and cybersecurity experts to maximize the chance of a positive outcome.

All County employees should understand this policy: do everything to prevent ransomware (be vigilant with emails and software updates), know that the County will support them with resources if an incident occurs, and know that we will simply not pay our way out of a cyber crisis. It's on all of us to make sure ransomware attackers find Geauga County a futile target.

Confidentiality of Cybersecurity Information (Public Records Exemption)

To facilitate open planning and thorough incident documentation without fear of sensitive information being exposed, Ohio law provides confidentiality for cybersecurity records. Under O.R.C. § 9.64(E), any records, documents, or reports related to the County's cybersecurity program or to any cybersecurity/ransomware incidents are exempt from Ohio's public records law. This means that such records are not subject to disclosure under O.R.C. § 149.43 (the Ohio Public Records Act). Geauga County will strictly uphold these confidentiality provisions in its handling of cybersecurity information.

Protected Records: The types of records covered by this exemption include (but are not limited to): the contents of this Cybersecurity Program and associated policies, risk assessment reports, network diagrams, security audits, incident response plans, incident logs and reports, communications about incidents, and any reports we submit to state authorities about incidents. These documents often contain highly sensitive details (system vulnerabilities, defensive measures, forensic

findings, etc.) which could be harmful if released to the public or potential attackers. By law, we can and will refuse public records requests for such information, citing O.R.C. § 9.64(E). This encourages County staff to be candid and comprehensive in writing reports and developing plans, knowing that they won't inadvertently hand a "blueprint" of our defenses to malicious actors. It also protects the privacy of individuals whose data might be discussed in incident reports.

Additionally, O.R.C. § 9.64(F) specifies that records identifying details of the County's cybersecurity systems (specific software, hardware, services, vendor names, etc.) are classified as "security records" under O.R.C. § 149.433 and are also exempt from disclosure. For example, if the County has documents listing what brand of firewall or anti-virus we use, or an inventory of security appliances, those are protected. The rationale is clear: divulging exactly which tools we use or are considering could help hackers tailor their attacks (e.g. exploiting known weaknesses of a product). So, information like product names, network architecture descriptions, and vendor contracts for security services will be treated as sensitive and kept confidential.

Handling of Requests and Information Sharing: All County personnel are instructed that if they receive any public records request that might encompass cybersecurity-related records, they should immediately refer it to the County Prosecutor's Office or legal counsel for review. The legal team will determine which records (or portions thereof) are exempt under these provisions and will respond by citing the appropriate exemptions (O.R.C. § 149.43(A)(1)(hh) for cybersecurity programs/incidents, and O.R.C. § 149.433 for security records). County employees should not release any documents pertaining to our cybersecurity program or incidents on their own. Internally, such documents are shared strictly on a need-to-know basis and are stored securely (with access controls in place). We will mark sensitive files as "Confidential – Security Sensitive" to prevent accidental sharing.

It is important to note that while these records are exempt from public disclosure, they are not exempt from oversight. The Auditor of State or other authorized oversight bodies may request to review our cybersecurity program and incident reports as part of audits or investigations. In those cases, we will comply and provide the information to the auditors or inspectors, who themselves are bound to confidentiality by law. Similarly, reports to state Homeland Security or OCIC are not public records in their hands either – the exemption follows the information. This statutory protection enables full transparency between the County and state cybersecurity authorities without risking public exposure.

By explicitly recognizing and invoking these public records exemptions in our program, Geauga County ensures two outcomes: (1) We encourage thorough documentation and honest self-assessment in cybersecurity (nothing will be swept under the rug for fear of headlines, because incident details remain internal), and (2) We prevent adversaries from exploiting our openness against us. The County's public messaging about cybersecurity will, of course, still promote citizen awareness and reassurance, but the granular details (like which server was hacked, or which software is deployed) will remain confidential for security's sake. This approach is fully compliant with O.R.C. 9.64(E) and (F) and aligns with standard security practice to keep sensitive security details on a strictly need-to-know basis. In summary, all records pertaining to this cybersecurity program or any cyber incidents will be securely maintained by the County and will not be released publicly, ensuring that our security posture is not compromised by unnecessary disclosure.

Roles, Responsibilities, and Enforcement

Governance Structure: Geauga County's cybersecurity governance involves multiple layers. The Board of County Commissioners, by adopting this program, provides top-level endorsement and resources for cybersecurity. The Automatic Data Processing (ADP) Board – chaired by the County Auditor and including representatives of key County offices – is responsible for establishing IT policies and overseeing their implementation across all County departments (as empowered by O.R.C. § 307.84 and 307.847). The ADP Board, through the Department of Advanced Technology and Applications (DATA) and the Department of Advanced Research and Cybersecurity (DARC), will administer the Cybersecurity Program on a day-to-day basis. The County Auditor (Chief Administrator of ADP) and Deputy Chief Administrator have authority to enforce compliance with these security policies, including the ability to restrict network access for any office or user that poses a security risk. They will also regularly report to the Board of Commissioners and the ADP Board on the state of the County's cybersecurity (e.g. summarizing risk assessments, training completion rates, and any notable incidents). This ensures that elected officials remain informed and engaged in supporting cybersecurity initiatives.

Departmental Responsibilities: Every County Office, Board, and Agency is responsible for complying with the Cybersecurity Program and related policies. Offices, Boards, and Agencies must ensure their staff complete the required training, follow the Acceptable Use rules in daily operations, and cooperate with ADP on security measures (such as installing updates or using MFA). If an entity plans to implement a new software system or process that could impact security, they are required to involve ADP in the planning to ensure compliance with this program (this is supported by O.R.C. § 307.847, which requires ADP Board approval for new IT purchases to maintain security standards). Entities should designate a security point-of-contact who works with ADP on incident response and disseminate security information to their staff. In the event of an incident, affected departments must fully cooperate with the DARC incident team, including providing access to systems and information needed to investigate and respond.

Individual Responsibilities: Each County employee and official is a critical participant in our cybersecurity efforts. Individuals are expected to:

- Adhere to all rules in the Acceptable Use Policy when using County devices or data (e.g. no installing unauthorized software, no connecting unapproved devices to the network, no sharing of passwords).
- Use strong passwords and multi-factor authentication as mandated, keeping their credentials secure.
- Be vigilant for phishing or suspicious activity and report anything unusual to ADP immediately (better to have false alarms than missed real threats).
- Complete all required cybersecurity training courses and exercises by the deadlines.
- Read and follow any additional security guidance or bulletins provided by ADP (for example, instructions during an active threat or updated procedures).
- Understand their role in incident response: know who to call or what to do if they suspect a cybersecurity incident (for most employees, this simply means call the ADP Service Desk or DARC if something seems very wrong, like a strange ransom note on screen).

By fulfilling these responsibilities, individuals greatly contribute to the County's overall security and help protect themselves and the community from harm.

Enforcement and Compliance: Compliance with the Cybersecurity Program is mandatory. The ADP Board and County leadership will enforce this policy through several mechanisms:

- **Technical Controls:** ADP DARC will implement technical enforcement where possible (for instance, systems will be configured to require MFA, password policies will be enforced in system settings, and devices that are not updated or running required security software may be automatically quarantined from the network).
- **Monitoring and Auditing:** Regular audits will be conducted to verify compliance (e.g. checking that all active accounts have MFA, scanning for unauthorized devices, reviewing access logs for policy violations). The Auditor of State's IT audit as well as internal audits will include checks for adherence to these policies. Any deficiencies or findings will be addressed with corrective action plans.
- **Incident of Non-Compliance:** If an employee or department is found to be in violation of cybersecurity policies (for example, an employee refusing to do training or a department circumventing security protocols), the issue will be escalated. Minor first-time issues may result in a warning and re-training. Serious or repeated violations may lead to disciplinary action in accordance with HR policies (which could include suspension of computer privileges or even employment consequences, depending on severity). For elected officials or independent offices, the ADP Board may take actions within its authority (such as restricting network connectivity for an office that refuses to comply, as a means to protect other County systems). The goal is not punishment for its own sake, but to mitigate risks immediately – for instance, if someone's account is compromised due to negligence, that account will be disabled until security is restored and the person is retrained.
- **Support and Resources:** The County will provide ample support to achieve compliance – including training resources, IT assistance, and clear guidance. We understand that policies can be complex, so ADP will help departments implement required controls and will be available to answer questions or provide hands-on help (like setting up MFA on devices). By making compliance as straightforward as possible, we expect fewer issues.

Review and Updates: This Cybersecurity Program is a living document. It will undergo a formal review at least annually and after any major cybersecurity incident or change in law. Updates will be proposed by the ADP staff and vetted by the ADP Board. This ensures the program remains up to date with evolving threats, technologies, and compliance requirements. The County will also take into account recommendations from external auditors, the Ohio OCIC, and lessons learned from exercises or incidents in updating the program.

Adoption as Official Policy: This document, upon approval by the Board of County Commissioners, becomes an official County policy manual for cybersecurity. All County offices are expected to adopt it as their own policy framework for cyber defense. The Board's adoption signals to all stakeholders – employees, residents, and potential attackers – that Geauga County takes cybersecurity seriously and is unified in this effort. Any prior policies or directives that conflict with this

program are superseded by it. However, all previously existing complementary policies (as listed in the integration section) remain in effect and are reinforced by this overarching program.

In conclusion, through clear roles and robust enforcement, Geauga County will maintain a strong Cybersecurity Program in compliance with O.R.C. § 9.64 and aligned with the highest standards. Cybersecurity is now an essential part of public service, and everyone in Geauga County government has a part to play in protecting our community's digital frontiers. By working together under this program, we will significantly reduce risk, respond effectively to challenges, and continue to serve the public with integrity and resilience in the face of cyber threats.

Appendix A – ORC § 9.64 Compliance Matrix

O.R.C. § 9.64 Requirement	Geauga County Implementation	CIS Control Reference
Identify critical functions, systems, and cybersecurity risks	DARC performs periodic risk assessments to identify critical County systems, functions, and vulnerabilities. These are documented and reviewed annually, with updates provided to DATA and CARE for implementation and records protection.	CIS Control 4 – Secure Configuration; CIS Control 12 – Network Infrastructure Management

Assess potential impacts of a cybersecurity breach	Risk assessments include business impact analyses (BIA) to determine potential service disruptions and public safety concerns. CARE ensures that critical records recovery timelines are defined.	CIS Control 14 – Security Awareness and Skills Training; CIS Control 17 – Incident Response Management
Implement threat detection and incident response procedures	Geauga County Policy on Reporting and Escalating Cyber Events establishes procedures for identifying, containing, and remediating security incidents. DARC maintains a 24/7 contact protocol for critical threats.	CIS Control 8 – Audit Log Management; CIS Control 17 – Incident Response Management
Establish recovery and infrastructure repair procedures	DATA coordinates with DARC to restore systems after incidents, using secure backups and validated recovery plans. CARE ensures archival data restoration processes are followed.	CIS Control 11 – Data Recovery; CIS Control 13 – Network Monitoring and Defense
Provide annual cybersecurity training for all employees	Annual security awareness training is mandated in the Geauga County Cybersecurity Awareness Training Policy ADP-25-F-006, with tracking by DARC. Free state-provided training (O-PCI) is utilized when appropriate.	CIS Control 14 – Security Awareness and Skills Training
Report incidents to Ohio Homeland Security (7	Incident reporting timelines and responsibilities are defined	CIS Control 17 – Incident Response Management

days) and Auditor of State (30 days)	in the Policy on Reporting and Escalating Cyber Events. DARC ensures compliance with both deadlines.	
Prohibit ransomware payments without legislative approval	In accordance with O.R.C. § 9.64(B), ransom payments require a formal resolution by the Board of County Commissioners. Default policy is non-payment unless expressly authorized.	CIS Control 11 – Data Recovery; CIS Control 17 – Incident Response Management
Protect cybersecurity program records from public disclosure	Under O.R.C. § 9.64(E), program documents, security configurations, and incident reports are classified as security records exempt from Ohio public records law.	CIS Control 3 – Data Protection

Signed by:
Charles Walder
5ECDE9230E05438...

Charles E. Walder, Geauga County Auditor

Automatic Data Processing Board Chief Administrator

9/10/2025 | 08:36:59 EDT

Date

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

Geauga County Cybersecurity Policy

ADP-25-F-003

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

The purpose of this policy is to establish comprehensive cybersecurity requirements and best practices for all Geauga County information systems and data. This policy applies to all agencies under the technology management of the Geauga County Automatic Data Processing Board (ADP). By aligning with the Center for Internet Security (CIS) Critical Security Controls, this policy aims to protect the County's internal systems and public-facing services, ensure the confidentiality, integrity, and availability of County data, and reduce cybersecurity risks to County operations and citizens.

Sec. 4.0 – Authority

This policy is issued under the authority of the Geauga County Automatic Data Processing Board which provides technology services under Ohio Revised Code 307.84. The County Auditor, as Chief Administrator of the ADP Board, oversees IT governance and security in accordance with Ohio law. Furthermore, this policy is designed to satisfy emerging state cybersecurity requirements: the Ohio Department of Administrative Services (DAS) has established minimum cybersecurity standards for local governments' systems and networks (including mandates for encryption, multi-factor authentication, patch management, logging/monitoring, incident response planning, and vendor security). Compliance with this policy also aligns with the Ohio Auditor of State's IT General Controls expectations and will help the County meet audit and regulatory obligations.

Sec. 5.0 – Policy and Procedure

The following security controls and procedures are hereby established for Geauga County's internal networks, systems, and public-facing services. All covered persons (see Sec. 1.0) must adhere to these requirements. Department heads and IT system owners are expected to implement these controls in their areas, and ADP will provide guidance and oversight.

Sec. 5.1 – Inventory and Control of Assets

- **Hardware Asset Inventory:** All computing devices and network-connected equipment (enterprise assets) must be actively inventoried and tracked. The inventory shall include end-user devices (desktops, laptops, tablets, mobile phones), servers, network devices (routers, switches, firewalls, access points), Internet of Things (IoT) devices, and any other device connected to County networks or cloud services. Unmanaged or unauthorized devices must be identified and removed or isolated promptly to prevent insecure devices from threatening the network.
- **Software Asset Inventory:** All software and applications installed or in use on County systems must be cataloged and authorized. This includes operating systems, server and network device firmware, desktop applications, mobile apps, cloud services, and any other software. Software not approved or no longer needed should be removed or disabled to prevent unauthorized or potentially malicious software from executing. ADP shall maintain the central asset inventory systems and provide tools/processes for departments to report new assets or changes. Periodic audits of hardware and software inventories will be conducted to ensure accuracy and completeness.

Sec. 5.2 – Secure Configuration of Systems
All County-owned technology assets must be configured according to security best practices to minimize vulnerabilities. Standard secure configuration baselines (such as CIS Benchmarks or vendor best practices) should be applied to servers, workstations, mobile devices, network devices, and applications. Key requirements include:

- **Operating Systems & Software Configuration:** Default passwords, unnecessary services, and default accounts must be removed or disabled. Systems should run with only essential services and software to reduce attack surface. Secure baseline configurations must be documented and consistently applied to new installations and updates. Any deviations or configuration changes must go through a change control process managed by ADP.
- **Network Device Configuration:** Firewalls, routers, switches, and wireless access points must be securely configured with appropriate access control lists, encryption, and up-to-date firmware. All remote management interfaces should use secure protocols and be accessible only by authorized administrators over secure channels. Default settings on network equipment (community strings, SNMP, etc.) should be changed and hardened during deployment.
- **Secure Configuration Management:** ADP will maintain configuration standards and checklists. Automated configuration management tools may be used to enforce settings and to regularly scan for configuration drift or non-compliance. Any configuration that is found to be insecure or non-standard must be corrected or documented via an approved exception. Systems must also be monitored for unauthorized changes.

Sec. 5.3 – Access Control and Account Management
Access to County systems and data must be strictly controlled. The principle of least privilege shall be employed: users and administrators should receive only the minimum access rights needed to perform their job functions. This section covers user account management, authentication requirements, and account monitoring:

- **Account Provisioning and Removal:** All user accounts (including employee, contractor, and service accounts) must be created following a formal process with management approval. Accounts should be tied to a unique individual or role; shared/generic accounts are prohibited unless absolutely necessary for a specific function (and if used, must be closely monitored). Account privileges (e.g. group memberships, administrative rights) should be assigned based on role-based access control. When personnel leave or contracts end, their accounts must be disabled or removed in a timely manner (generally within 24 hours of separation). Periodic reviews (at least quarterly) of user and administrator accounts shall be performed by ADP and department heads to disable any inactive or unnecessary accounts.
- **Authentication (Passwords and MFA):** All accounts must be secured with strong authentication. **Multi-Factor Authentication (MFA)** is required for all County domain accounts, email (Microsoft 365) accounts, and any other accounts used to access sensitive systems or data. Users must authenticate with at least two factors (e.g. a secure password plus an approved hardware or software token). Passwords must meet the complexity and length requirements defined in the Geauga County Multi-Factor Authentication and Password Policy (Policy #28-22-018) – currently a minimum of 25 characters with a mix of character types. That policy is incorporated by reference into this cybersecurity policy, and all users are expected to comply with its standards for password creation, rotation (if applicable), and MFA usage.
- **Account Monitoring and Management:** ADP will utilize tools to monitor account usage and login activities. Suspicious logins or access attempts (e.g. repeated failed logins, login from unusual locations) should trigger alerts for investigation. Service accounts and accounts with elevated privileges (administrators) must be monitored closely. Any default or vendor-supplied accounts on systems must either be deleted or, if required for operation, renamed and secured. ADP will conduct periodic audits of accounts and privileges to ensure compliance with this policy and will remove or adjust any access that is not justified.

Sec. 5.4 – Continuous Vulnerability Management
The County shall continuously identify, assess, and remediate vulnerabilities in its IT environment to minimize the window of opportunity for attackers. A formal vulnerability management program will be maintained, including the following elements:

- **Vulnerability Scanning:** ADP will run regular vulnerability scans of internal networks, servers, workstations, and public-facing systems (e.g., websites, citizen portals) using approved scanning tools. Scans should be conducted at least monthly on internal systems and more frequently (e.g., weekly) on critical external systems, or whenever significant new vulnerabilities (zero-days) emerge that could affect the County. Vulnerability scan reports will be reviewed and high-risk findings will be prioritized for prompt remediation.
- **Patch Management:** Timely patching of operating systems, software, and firmware is required to address known vulnerabilities. Critical and high-severity patches should be applied as soon as practical (for example, within 14 days of release, or sooner if active exploits exist). All county systems (servers, endpoints, network devices, applications) must regularly receive security updates. ADP will maintain an enterprise patch management process

and schedule and verify that updates are applied successfully. Systems that cannot be patched immediately due to operational constraints must have mitigating controls (such as network isolation or additional monitoring) and a documented timetable for patching.

- **Configuration of Vulnerability Alerts:** The IT security team will subscribe to threat intelligence and vendor security bulletins (from sources such as MS-ISAC, CISA, software vendors). This ensures awareness of newly disclosed vulnerabilities or threats that could impact the County. When credible alerts are received, the team will assess impact and, if needed, perform out-of-cycle scans or patches.
- **Remediation and Tracking:** Detected vulnerabilities shall be logged and tracked to closure. The vulnerability management program will include defined timelines for remediation based on severity (e.g., critical findings fixed within 7 days, high within 30 days). Department IT liaisons and system owners are expected to coordinate with ADP to test and apply patches or fixes. Verification scanning will be performed to confirm that vulnerabilities have been resolved.

Sec. 5.5 – Audit Log Management and Monitoring
The County will collect and retain audit logs of security-relevant events from systems, applications, and network devices to help detect and investigate incidents. Effective log management and monitoring includes:

- **Logging of Key Events:** Systems must be configured to log significant events, including (but not limited to) user login attempts (successful and failed), account creations/deletions, privilege changes, system startups/shutdowns, configuration changes, security alerts (antivirus, IDS/IPS), and access to critical data. For applications and databases that hold sensitive information, log access to those records as feasible.
- **Centralized Log Collection:** Whenever possible, logs from servers, workstations, network devices, and major applications should be forwarded to a centralized Security Information and Event Management (SIEM) system or log server maintained by ADP. Centralizing logs allows correlation and analysis across the enterprise and secure retention of logs.
- **Log Retention:** Audit logs will be retained in accordance with County policy and regulatory requirements. At minimum, security logs should be retained for a sufficient period (e.g., 1 year or longer for critical systems) to support investigations and audits. Archived logs should be protected from unauthorized access or tampering.
- **Monitoring and Review:** IT security personnel (or designated managed security service providers) will regularly review logs and automated alerts for signs of malicious activity or policy violations. The County may employ automated intrusion detection/prevention systems (IDS/IPS) and log analytics tools to generate alerts on suspicious patterns (e.g. multiple failed logins, unusual after-hours access, high-volume data transfers). Any detected incident or anomaly will be investigated per the Incident Response procedure (Sec. 5.10). Administrative account activities and remote access logs should be given particular attention in reviews.

Sec. 5.6 – Email, Web, and Malware Protection
Email and web usage are primary vectors for cyber threats (phishing, malware, etc.) and pose a critical risk to County operations. The County will implement layered defenses to protect against threats from email and web content, including:

- **Email Security:** All County-provided email accounts (e.g., Microsoft 365 email) will have enterprise email security controls. This includes spam filtering, malware/virus scanning of attachments, and phishing protection (such as malicious link scanning or blocking). Users should be trained to recognize phishing emails and report

suspicious messages. Email authentication technologies like DMARC, DKIM, and SPF should be implemented on County email domains to prevent spoofing.

- **Web Browser Protections:** County computers should have safe browsing tools or filters enabled to block access to known malicious websites. Web traffic may be filtered and monitored to prevent downloads of malicious content. Up-to-date browser software and plugins are required; unsupported or vulnerable browser plugins should be removed or disabled. Where feasible, use of ad-blocking and script-blocking extensions is encouraged to reduce risk from web ads or scripts. Only ADP approved web browsers and browser extensions should be used.
- **Malware Defenses on Endpoints and Servers:** All County-owned endpoints (desktops, laptops, mobile devices) and servers must run approved Endpoint Detection and Response (EDR) software. Anti-virus definitions and threat intelligence feeds should be kept current (with updates applied at least daily). The EDR solution should be centrally managed by ADP to ensure consistent policy enforcement and to receive alerts on detections. In addition, application whitelisting or restricting software execution to approved programs should be considered for critical systems to prevent unauthorized code from running.
- **Removable Media and Downloads:** Usage of removable media (USB drives, etc.) should be controlled; such media should be scanned for malware before use on County systems. Users are not permitted to use personal USB drives or other removal media on County systems. Users are discouraged from downloading software or files from untrusted Internet sources. If downloads from unverified sources are necessary for business, they must be scanned and/or executed in a sandboxed environment first whenever possible.
- **Email and Web Usage Policy:** (Refer to the County's Acceptable Use Policy if applicable.) Users should not use County email or internet access for high-risk activities. Any email or website that is not work-related and seems suspicious should be avoided. Users must immediately report if they suspect a malware infection or if they clicked a suspicious link/attachment, so ADP can respond quickly.

Sec. 5.7 – Network Security and Public-Facing Services

The County's networks (including internal office networks, data center networks, and public Wi-Fi networks) must be secured to prevent unauthorized access and to protect public-facing services. This section covers network infrastructure management, secure network architecture, and specific controls for public services:

- **Network Infrastructure Management:** All network devices (firewalls, routers, switches, wireless controllers, etc.) must be actively managed and kept up to date by ADP. Configuration changes on critical network devices should follow change management and be performed by authorized network administrators. Default administrative passwords on network equipment must be changed, and management interfaces should be accessible only over secure channels (SSH, HTTPS) and preferably only from the internal management network or via VPN. Unnecessary network services or ports should be disabled to harden the devices. Regular audits of firewall rules and network device configurations will be conducted to ensure they meet security requirements.
- **Network Segmentation:** The County shall implement network segmentation to separate and protect sensitive systems. For example, internal government networks should be separated from any public-access networks; law enforcement or other high-sensitivity departments may have isolated network segments or VLANs. Critical servers (e.g., databases with resident data) should reside in restricted zones accessible only by authorized systems/users. Proper network segmentation limits the reach of an attacker should a breach occur in one area.
- **Public Wi-Fi and Guest Network:** Public or guest Wi-Fi networks (such as those provided in County facilities for citizens) must be completely segregated from the County's internal operational network. Public Wi-Fi should

be on its own VLAN or network, with strict firewall rules preventing access to internal resources. Users of public Wi-Fi should not be able to reach internal County systems. Additionally, public Wi-Fi should require acceptance of terms of use and possibly use client isolation so that public users cannot attack each other. The County should apply web filtering on public Wi-Fi to block malicious sites or inappropriate content as necessary.

- **External Facing Systems:** All public-facing systems (e.g., County websites, citizen service portals, online payment systems) must be designed and maintained with security in mind. These systems should reside in a DMZ or cloud environment with strong perimeter controls. Web application firewalls (WAFs) should be used for critical web services to detect and block common web attacks. All external-facing applications must use HTTPS encryption for all user communications (enforcing TLS for data in transit). Administrative interfaces for these systems should **not** be exposed to the public internet; they should be accessible only through secure channels (VPN or internal network). Regular vulnerability scanning and penetration testing (see Sec. 5.13 and 5.14) will be performed on public-facing applications to identify and remediate security issues.
- **Wireless Networks:** Besides public Wi-Fi, any internal wireless networks used by County staff must enforce strong encryption (WPA2 or WPA3 Enterprise with authentication) and should be segmented like any other network. Wireless access points should be configured to prevent unauthorized devices from connecting (e.g., using certificate-based authentication or managed via a central controller that can disable rogue APs). Regular wireless security assessments should be conducted to detect any rogue access points or unauthorized wireless devices.

Sec. 5.8 – Data Protection and Encryption

Geauga County must protect sensitive data against unauthorized access or loss. The County will develop processes and technical controls to identify and classify its data, and to handle data securely throughout its lifecycle. Key data protection requirements include:

- **Data Classification:** All County data should be classified by sensitivity (e.g., Public, Internal, Confidential, Highly Sensitive). Examples: public records and website content can be Public; internal communications might be Internal; personal identifiable information (PII) about citizens or employees, financial records, or law enforcement data would be Confidential or Highly Sensitive. The classification will determine the handling standards for the data. Department directors in coordination with ADP will define data categories and ensure data in their custody is labeled and handled according to its classification.
- **Access Control to Data:** Access to sensitive data (digital or physical) must be restricted to authorized personnel only. Systems storing confidential information should implement access controls such as user permissions, encryption, and auditing of access. Where possible, employ data loss prevention (DLP) technology to prevent unauthorized sharing or exfiltration of sensitive data (for instance, blocking emails or uploads containing SSNs or other PII unless authorized).
- **Encryption:** Sensitive data must be encrypted both at rest and in transit. “At rest” means when stored on devices or media (servers, databases, laptops, backups, USB drives), the data should be encrypted using strong encryption algorithms. Full-disk encryption should be enabled on County laptops and mobile devices to protect against theft. For servers and databases, file-system or database encryption should be used for sensitive fields. “In transit” means whenever data is transmitted over a network (for example, between a user and a web application, or between two systems), industry-standard encryption (TLS/SSL, VPN tunnels, etc.) must be used. Email containing confidential data should be sent through encrypted means or with email encryption solutions.

- **Secure Disposal:** When data is no longer needed or must be deleted (per retention schedules or legal requirements), it must be disposed of securely. For electronic data, this means using approved data wiping tools or cryptographic erasure; simply deleting files is not sufficient. For physical media (printed documents, disks, USB drives), shredding or incineration must be used as appropriate. Documentation of disposed records should be kept when required by record retention policies.
- **Handling of Personal and Confidential Data:** All workforce members must handle PII, financial information, health information, and other confidential data with care. Such data should not be stored on unapproved personal devices or transmitted through unauthorized cloud services. Wherever possible, minimize the collection and retention of sensitive data – collect only what is required for business needs and retain it only as long as necessary. Regular training (see Sec. 5.11) will be provided on proper data handling practices.

Sec. 5.9 – Data Backup and Recovery
To ensure continuity of operations and the ability to recover from incidents (such as ransomware or natural disasters), the County will establish and maintain robust data backup and recovery practices. Key points of the data recovery policy include:

- **Regular Backups:** All critical systems and data (servers, databases, essential documents, etc.) must be backed up on a regular schedule. The frequency of backups should align with the criticality of the data and Recovery Point Objectives (e.g., daily backups for most systems, with more frequent backups for highly critical databases if needed). Backups should include not only on-premises server data but also cloud-based data (e.g., data in Microsoft 365 or other cloud services) using suitable backup solutions.
- **Backup Protection:** Backup files and media must be protected with the same rigor as production data. Backups should be encrypted (especially if stored off-site or in cloud backup storage) to prevent unauthorized access. Access to backup repositories should be limited to backup administrators. At least one backup copy should be stored offline or in a manner that is isolated from the network (to protect against ransomware that might try to delete or encrypt backups). Backups should be immutable, if possible.
- **Testing of Restores:** Periodic recovery tests shall be conducted to verify that backups are functional and that data and systems can be successfully restored within acceptable time frames. At least annually (and preferably more often), ADP will perform test restores of a sampling of backups, including full system recovery and file-level recovery, to ensure the process works and data integrity is maintained. Any issues discovered during testing (e.g., corrupt backup, incomplete data) must be fixed promptly.
- **Business Continuity Alignment:** Each department should be aware of what data is being backed up and the expected recovery times. This ties into the County's broader disaster recovery and business continuity plans. Critical systems should have documented Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) that guide the backup strategy. In case of a major incident (cyberattack or otherwise), the County will prioritize restoration of services based on those plans.
- **Data Archival and Retention:** Backup and recovery procedures will comply with any data retention requirements mandated by law or policy. Data that needs to be retained long-term (for legal or historical reasons) may be archived to secure, durable storage. Such archives should also be backed up or replicated. Expired backups that are no longer needed should be securely deleted to free storage and protect data (especially if they contain sensitive information).

Sec. 5.10 – Incident Response and Management
Despite preventive measures, security incidents may occur. Geauga County will maintain an Incident Response (IR) capability to rapidly detect, contain, and recover from cybersecurity incidents. This includes having policies, plans, procedures, defined roles, and training for incident handling. Key aspects of the incident response program are:

- **Incident Response Plan:** The County shall have a written Incident Response Plan that outlines the steps to take when a security incident is suspected or confirmed. The plan will define what constitutes an incident (e.g., malware infection, system breach, data leak, network intrusion), severity levels, and escalation criteria. It will also list key roles (Incident Response Team members) and their responsibilities during an incident. This policy document serves as a high-level directive; the detailed IR Plan maintained by ADP will align with this policy and be reviewed at least annually.
- **Incident Response Team and Roles:** A cross-functional Incident Response Team (IRT) will be designated. This may include members from ADP (security analysts, system/network admins), legal, public relations, management, and affected department representatives. ADP's CISO, Director of DARC, or designee will typically serve as Incident Coordinator. Roles such as Communications Lead (to handle internal/external communication), and a Liaison to law enforcement or third-party response services (e.g., Ohio State cyber incident support) should be established.
- **Detection and Reporting:** All users and staff have a responsibility to report signs of a potential security incident immediately (for example, unusual system behavior, suspected phishing emails, lost/stolen devices, or evidence of data leakage). ADP will maintain monitoring systems (per Sec. 5.5 and 5.7) to detect threats. A centralized 24/7 incident reporting mechanism (such as a security hotline or email) will be available.
- **Response Procedures:** Upon identifying an incident, the IRT will follow a standardized process: **Preparation**, **Identification**, **Containment**, **Eradication**, **Recovery**, and **Lessons Learned**. Specific actions include isolating affected systems (to contain spread of malware or prevent further unauthorized access), collecting forensic evidence if applicable, neutralizing the threat (e.g., removing malware, shutting down accounts or services being abused), restoring systems from clean backups (see Sec. 5.9) and verifying the systems are secure (patches applied, vulnerabilities closed). Communications during an incident will be managed carefully, including any required notifications (to law enforcement, affected individuals if personal data was breached, Ohio state authorities, etc., per legal requirements).
- **Incident Documentation:** All incidents and responses must be documented in an incident tracking system or report. Documentation should include timelines of events, actions taken, communications made, and final resolution. This helps with post-incident analysis and demonstrates due diligence to auditors or authorities if needed.
- **Post-Incident Activity:** After an incident is resolved, the IRT will conduct a "lessons learned" review to analyze what happened and how to improve. They will identify any gaps in controls or response and develop an action plan to address them (such as additional training, new tools, or changes in procedures). Significant incidents and lessons will be reported to the ADP Board and County leadership. The incident response plan and related procedures will be updated, if necessary, based on lessons learned.

Sec. 5.11 – Security Awareness and Training
Technology alone is not sufficient; users must be aware of cybersecurity best practices and threats. Geauga County will

establish and maintain a security awareness training program to ensure all workforce members have the knowledge and skills to protect County information. Key elements include:

- **New Hire Training:** All new County employees, contractors, or others with access to County IT resources must complete basic security awareness training as part of orientation. This training will cover the County's security policies, proper use of IT resources, how to identify and report common threats (phishing, social engineering, etc.), and user responsibilities in keeping systems secure.
- **Ongoing Awareness Activities:** At least annually, all personnel must complete a refresher cybersecurity training course. The training content will be updated regularly to include emerging threats and any changes in policy or procedures. In addition to formal training, the County will provide ongoing awareness materials such as email bulletins, posters, and cybersecurity tips to reinforce good practices (for example, reminders to not share passwords, to lock screens, to be cautious with email attachments).
- **Phishing Simulations:** The IT security team may conduct periodic simulated phishing exercises to gauge user awareness and adherence to training. Users who fall for simulated phishing emails will be notified and may receive additional targeted training. The goal is to improve vigilance against real phishing attacks, which are a common threat to local governments.
- **Role-Based Training:** Staff in specialized roles (e.g., IT administrators, incident response team members, helpdesk, or anyone with privileged system access) will receive additional training tailored to their security responsibilities. For instance, system administrators may receive training on secure configuration and incident handling relevant to systems they manage. Similarly, developers of any in-house web applications may receive training on secure coding practices (as related to Sec. 5.12).
- **Tracking and Compliance:** ADP (or HR department in coordination) will track completion of required training. Compliance with security training is mandatory; failure to complete training may result in disciplinary action or loss of system access. The importance of security awareness will also be emphasized by County leadership to foster a culture of security.

Sec. 5.12 – Application Security and Development
For any software applications developed in-house or configured by the County (including citizen-facing web portals, mobile apps, or internal workflow applications), as well as third-party applications used by the County, security must be integrated into their lifecycle. The goal is to prevent, detect, and remediate software vulnerabilities before they are exploited. Requirements include:

- **Secure Development Practices:** Developers (internal or contracted) must follow secure coding guidelines and best practices, such as CISA's Secure by Design principles. This includes validating inputs, avoiding known vulnerable functions, proper error handling (not exposing sensitive info), and implementing authentication and session management correctly. Web applications should be developed to defend against common threats like SQL injection, cross-site scripting (XSS), CSRF, etc. (following OWASP guidelines). Before deployment of new applications or major updates, a code review or security assessment should be conducted to catch vulnerabilities early.
- **Third-Party Application Configuration:** Many County systems use off-the-shelf software or cloud services. These must be configured securely. Default admin passwords must be changed and unnecessary default accounts disabled. Optional security features provided by the software (such as enabling MFA, encryption, logging) should

be reviewed and turned on by administrators if feasible, with security outweighing ease of use. Security should not be avoided just because it adds time or difficulty to a task. Application administrators are expected to work with ADP to ensure settings meet County security standards, and if an application has the capability for stronger security (like add-on modules for MFA or auditing), those should be implemented. If turning on a security feature is a concern due to the severe impact it has on operation or use, then ADP executive leadership should be consulted to accept or decline the risk associated with leaving the feature off.

- **Vulnerability Patching in Applications:** Just as with operating systems, applications (including web plugins, content management systems for websites, etc.) must be kept updated. Departments using specific software are responsible for monitoring vendor patches and applying them with support from ADP. Web applications should have all components (server software, frameworks, libraries) updated to fix security issues as they become known. If a critical vulnerability is announced in an application the County uses (for example, a library like Log4j), the application or library must be patched or mitigated swiftly, even if that means emergency updates.
- **Application Testing and Assessment:** The County will subject critical applications to periodic security testing. This could include automated vulnerability scanning of web applications, penetration testing (Sec. 5.14), and/or code analysis. Particularly for citizen-facing portals that handle sensitive data or payments, an independent security assessment or penetration test should be done before go-live and regularly thereafter. Findings from such tests must be remediated in a timely manner.
- **Change Management for Applications:** Changes to application code, configurations, or infrastructure must go through change control procedures. This ensures that updates are tested and approved and that there's a back-out plan if something goes wrong. It also provides an opportunity to ensure security is re-validated after changes.
- **Secure Acquisition:** When procuring new software or cloud services, the County must evaluate the security of the vendor and product (see also Sec. 5.13 on Service Provider Management). Contracts with software vendors should include security clauses (e.g., the vendor must patch known vulnerabilities, disclose breaches, etc.), and whenever possible, security requirements (such as support for SSO/MFA, compliance with standards like CJIS or HIPAA if applicable) should be part of product selection.

Sec. 5.13 – Service Provider and Vendor Management

Service providers that manage County IT systems or have access to sensitive data (e.g., cloud service providers, managed service providers, software vendors, consultants) must be vetted and managed to ensure they follow strong security practices. The County remains accountable for protecting its data even when using third parties. Requirements for managing vendors include:

- **Vendor Security Evaluation:** Before entering a contract with an IT service provider or vendor who will handle sensitive data or critical systems, the County (through ADP and Procurement) will perform due diligence on the vendor's security. This may involve reviewing the vendor's security policies, standards, audits/certifications (such as SOC 2 reports), and references. Only vendors that meet the County's security requirements or demonstrate a commitment to cybersecurity should be selected.
- **Contractual Security Requirements:** Contracts with IT vendors must include appropriate security and privacy clauses. This can include requirements for data protection (encryption, breach notification within a specific timeframe, etc.), compliance with relevant regulations, right-to-audit clauses, and requirements that the vendor maintain minimum cybersecurity practices (for example, the County may require the vendor to also follow CIS

Controls or maintain cyber insurance). If the vendor will have remote access to County systems, they must do so via secure methods and possibly use MFA as well.

- **Ongoing Oversight:** The County will maintain an inventory of its critical service providers. ADP will assign an owner to each vendor relationship to monitor performance and security compliance. Vendors should provide regular reports on security if applicable (e.g., annual penetration test results or audit certifications). Any significant changes in the vendor's security posture or any breaches they suffer must be communicated to the County immediately as per contract.
- **Access Management for Vendors:** Vendors or contractors who are given accounts to access County systems (for support or operations) fall under the same account management rules as internal users (Sec. 5.3). Their access should be limited to what is necessary and disabled when not in use. If a vendor is only needed temporarily, their accounts should be set to expire. All remote vendor access must be monitored and logged.
- **Third-Party Software Management:** For third-party software used by the County, ensure that support and updates are maintained. If a vendor goes out of business or stops supporting a product, the County should plan to replace or retire that software to avoid running unpatched, vulnerable systems. Also, if a service provider sub-contracts part of the service, the County must be informed, and those subcontractors should also meet equivalent security requirements.

Sec. 5.14 – Penetration Testing and Assessments

In addition to internal vulnerability scanning (Sec. 5.4) and other controls, the County will conduct periodic penetration testing or engage independent security assessments to evaluate the effectiveness of its cybersecurity measures. Such tests simulate the actions of real attackers and can uncover weaknesses in people, processes, or technology that other measures might miss. Key points include:

- **Scope of Testing:** Penetration tests should be performed on critical systems and networks, including both internal infrastructure and external/public-facing applications. This includes (but is not limited to) network pen-testing of County offices and data centers, web application testing for citizen portals or public websites, and social engineering tests (like phishing attempts against County staff) to gauge human vulnerability. Tests may be conducted by qualified in-house personnel or by external security firms.
- **Frequency:** At minimum, a comprehensive penetration test of the County's environment should be performed annually. High-risk or critical services may warrant more frequent testing (for example, a major web portal could be tested before each major release). Additionally, significant changes (like a new system launch or major upgrade) should prompt a new assessment.
- **Remediation of Findings:** Results of penetration tests will be documented in a report to ADP and relevant agency leadership. Each finding (security gap or vulnerability discovered) must be evaluated and assigned an owner for remediation. High-severity findings should be addressed as top priority. The County will develop a remediation plan for all findings and track the resolution. Penetration test results are sensitive and will be treated as confidential; however, summary results and remediation status may be reported to oversight bodies (like the ADP Board or State Auditor) as needed to demonstrate compliance and improvement.
- **Compliance and Assurance:** Penetration testing is one way to validate that the controls outlined in this policy are functioning effectively. It provides assurance to County leadership and to external auditors/regulators that we are proactively seeking out and fixing weaknesses. These tests will also help fulfill any state or federal

compliance requirements for regular security assessments (for example, if required under specific data protection laws or Ohio's cybersecurity standards).

Sec. 6.0 – Roles and Responsibilities

All Cybersecurity is a shared responsibility across the organization. The following roles and groups have specific responsibilities under this policy:

ADP: ADP is responsible for implementing and overseeing the technical controls in this policy. ADP will maintain asset inventory systems, manage network security devices, deploy and update security software (antivirus, scanners, etc.), and administer centralized systems like logging and backup solutions. ADP also develops and maintains the Incident Response Plan and provides cybersecurity training and support to all County agencies. ADP has the authority to enforce compliance, including the ability to disconnect or disable any system that poses a security threat. They will also coordinate with external entities (law enforcement, state cybersecurity resources, MS-ISAC) when responding to incidents or threats. Finally, ADP can grant exceptions to certain requirements in this policy, but only with documented justification and usually on a temporary basis (see "Policy Compliance" for the exemption process).

Department Heads and Elected Officials: Leaders of each County department or agency must ensure that their staff and systems comply with this policy. They are responsible for fostering a culture of security within their teams, ensuring employees complete required training, and allocating resources for necessary security measures (such as keeping software up-to-date or engaging in required assessments). Department heads should work with ADP when implementing new systems or services to ensure security is considered from the start. They must also promptly report any incidents or potential threats within their department to the ADP. If a department uses specialized software or has unique systems, the department head must designate an **Application/System Administrator** (who could be a departmental IT liaison or power user) responsible for that system's security and for coordinating with ADP on updates, MFA configuration, and other security features. Agencies and Departments that employ IT staff are responsible for maintaining and regularly updating their asset inventory list, including hardware, software, and services, and should coordinate with ADP to ensure accuracy. Agencies and Departments that do not employ IT staff should coordinate with ADP to verify inventory systems are kept up to date and accurate.

Users (All County Staff and Account Holders): Every user of County IT resources has a responsibility to follow cybersecurity policies and procedures. Users must utilize strong passwords and MFA as required and must not share their credentials. They should practice safe computing – for example, avoid clicking on suspicious links, use County email and internet for official use in line with policies, and secure their workstations by locking screens when away. Users are expected to report any lost or stolen device, or any suspected security incident or suspicious activity immediately to the ADP Service Desk, who will then coordinate with DARC. Compliance with this policy and related standards (like the

Password/MFA policy) is a condition of continued access to County systems; failure to comply may result in disciplinary action.

Application and System Administrators: For specific applications or systems (which might be managed at a department level or by a vendor), the designated administrators of those systems must ensure security controls are in place per this policy. For example, if an application offers an option to enable MFA or enhanced security settings, the system admin must configure it accordingly. They must keep the system updated/patched and work with ADP to address any vulnerabilities. If an application cannot technically meet a requirement (for instance, an older system that cannot enforce MFA or strong passwords), the administrator must inform ADP and seek guidance or an explicit exemption. Administrators are also responsible for controlling access rights within their systems (only granting access to authorized users, removing users who no longer need it) and for maintaining any local logs or audit trails for the system.

Automatic Data Processing Board (ADP Board): ADP Board, chaired by the County Auditor, provides governance and oversight for County IT initiatives and policies. The Board is responsible for reviewing and approving this cybersecurity policy and any significant updates. They ensure that the policy aligns with legal requirements and risk appetite. In their oversight role, the Board will receive periodic updates from ADP on the state of cybersecurity (including major incidents, audit results, and compliance status). The Board supports enforcement by backing necessary disciplinary actions or resource allocations to uphold security.

Auditor of State / External Auditors: (Note: While not an internal role, it's worth mentioning in context of responsibilities.) The Ohio Auditor of State's office or other external auditors may assess the County's adherence to IT general controls as part of regular audits. County IT and management must cooperate with auditors, provide evidence of compliance (policies, logs, training records, etc.), and address any audit findings related to cybersecurity. This policy and its implementation are intended to meet the Auditor's standards for IT controls, thereby reducing the risk of audit findings.

Sec. 7.0 – Policy Compliance and Enforcement

1. **Compliance Monitoring:** Geauga County ADP will verify compliance with this policy through various methods, including but not limited to periodic walk-throughs, technical audits, network monitoring, vulnerability assessment reports, and review of user access logs. ADP may conduct random or scheduled audits of department systems to ensure security configurations and procedures align with this policy. ADP will also utilize automated tools (for example, to check for weak passwords, missing patches, or insecure configurations) as part of ongoing compliance checks. If any deficiencies or deviations are identified, ADP will inform the relevant department and work with them on a remediation plan with a defined timeline.
2. **Enforcement:** All individuals and departments covered by this policy are expected to comply with its requirements. Non-compliance or violations of this policy may result in serious consequences. Any business unit or department found to be in violation may face temporary restrictions, such as removal from the network or delays in IT services, until compliance is achieved. Individuals who intentionally disregard or repeatedly fail to follow this policy may be subject to disciplinary action by County management, up to and including termination

of employment. For vendors or contractors, violations could lead to termination of contracts or legal action as appropriate. The County will enforce this policy consistently to protect its assets and data.

3. **Alignment with Auditor Standards:** Adhering to this policy will help ensure the County meets the Ohio Auditor of State's IT general control standards. Lack of compliance can lead to negative audit findings and other repercussions. Notably, Ohio's new cybersecurity mandates tie compliance to potential funding and liability outcomes – non-compliance can result in auditor findings, funding consequences, increased insurance costs or denial of cyber insurance claims, as well as greater risk of data breaches and legal liability for the County. All County officials should recognize that cybersecurity is now a key component of regulatory compliance and good governance.
4. **Exceptions and Exemptions:** In rare cases, a specific control in this policy may not be immediately attainable due to technical limitations or extraordinary circumstances. Departments requiring temporary exemption must submit a written request to ADP explaining the justification. ADP executive leadership, possibly in consultation with the ADP Board, will review the request and may grant a limited, documented exemption with compensating controls in place if appropriate. All exceptions will include an expiration or review date. Permanent exemptions are discouraged and would require high-level approval. The existence of an exception does not exempt the department from working towards an alternative solution; it is expected that all feasible efforts will be made to ultimately comply with the policy requirements.
5. **Review and Revision:** This cybersecurity policy should be reviewed on a regular basis (at least annually, or more frequently if required by changes in law or the IT environment). Reviews will be coordinated by ADP and approved by the ADP Board. Revisions may be made to address new threats, changes in CIS Controls, or lessons learned from incidents and audits. All significant changes will be communicated to County employees and relevant parties. The *Issued/Revised/Reviewed* dates in Sec. 2.0 will be updated accordingly to document the policy lifecycle.

By order of the Geauga County Automatic Data Processing Board, this policy is effective as of the issuance date above. All County agencies and personnel are expected to familiarize themselves with its contents and integrate these cybersecurity practices into their daily operations. Through collective adherence to this policy, Geauga County will maintain a strong defense against cyber threats and protect the services and information relied upon by our citizens.

Sec. 8.0 – Policy Revisions

ADP will review this policy periodically (at least annually or as needed) and update it to reflect new threats, technologies, or compliance requirements. All revisions will be documented and communicated to stakeholders.

Below is the revision history for this policy:

Signed by:
5ECDE9230E05438...

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

7/17/2025 | 08:14:42 EDT
Date

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:

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

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

Date

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

Multi-Factor Authentication and Password Policy

Sec. 1.0- Applies To

1. Geauga County end users, employees, management, elected officials, technical support staff and team members.
2. Contractors, vendors or affiliated entities who are given a domain account or any other accounts provided by the county.

Responsible Office Geauga County ADP-DOIT Department of Information Technology

Classification Level: Public

Sec. 2.0- Policy

Issued: 06/15/2022
Revised: 06/15/2022
Reviewed: 06/15/2022

Multi-Factor Authentication (MFA) is an authentication method used to provide greater security for an account by requiring the use of multiple authentication methods in order to login and continue using an account. Proper MFA will use at least two of the three factors of authentication but may use more: Something you know (ex: password), something you have (ex: token, authenticator app), something you are (biometrics).

MFA follows a security framework called Zero Trust, where all users must be authenticated before (and continue to be authenticated while) having access to computers, networks, applications or data. Traditionally, but archaically, organizations would use the "Trust but verify" method of security, where users were trusted by default and only need to verify, usually by a password. This puts an organization at risk from internal bad actors, cracked passwords, and stolen credentials. By implementing MFA and Zero trust, we will reduce risk to the County network, applications and ensure we are protecting the County's Data.

Passwords can be easy to crack. The web is full of tools and programs that can easily allow a bad actor to steal your password simply by using "brute force." Short non-complex passwords can be broken instantly or within a couple minutes but, by extending the password length and complexity, can move that time to break into hours, days or even years. Most bad actors do not have the time or resources to break passwords of considerable length and complexity and so we can protect ourselves by following those practices.

Sec. 3.0- Purpose of the Policy

The purpose of this policy is to establish requirements, use and best practices for Multi-Factor Authentication and Passwords that all agencies must follow under the technology management of the Geauga County ADP-DOIT Department of Information Technology.

Sec. 4.0- Authority

The Geauga County Department of Information Technology (ADP-DOIT-DoIT) provides technology services under O.R.C. 307.84 to agencies and other county customers in Geauga County, its sixteen townships, and municipalities in Northeast Ohio. Those services include hosting, network, telecommunications, desktop computing, project management services, unified communications such as email, calendaring, team collaboration, and information security management, among others.

The Department operates under the leadership of the County Auditor, Mr. Chuck Walder who also serves as the Secretary and Chief Administrator of the Automatic Data Processing Board. The County Auditor's Office is created by State Statute. As such, the County Auditor is independently elected by the voters within the County and the County Auditor is governed by the laws of the State of Ohio, which have been approved by the Ohio Legislature and Ohio's Governor.

Sec. 5.0- Policy and Procedure

Sec. 5.1- Domain

1. The following applies to all domain users on Geauga Information Systems (GIS) domain, GIS child domains, domains in a trust relationship with GIS and any other domains in which ADP manages.
    a. Multi-Factor Authentication must be setup and used on all domain accounts.
    b. A minimum of two factors of authentication must be used.
        i. The first factor must be a secure password using 3 out of the 4 following options: number, lower case letter, capital letter, special character. The password must also be a minimum of 25 characters in length.
        ii. The second factor must be a hardware token. Approved hardware tokens are Gatekeeper and YubiKey.
        iii. ADP reserves the right to add or remove acceptable factors of authentication.

Sec. 5.2- Email and Microsoft 365

1. The following applies to all who users who have a Microsoft 365 account provided by ADP.
    a. Multi-Factor Authentication must be setup on all M365 accounts.
    b. A Minimum of two factors must be used.
        i. The first factor must be a secure password using 3 out of the 4 following options: number, lower case letter, capital letter, special character. The password must also be a minimum of 25 characters.
        ii. The second factor must be Microsoft Authenticator app.
        iii. ADP reserves the right to add or remove acceptable factors of authentication.

Sec. 5.3- All Other Applications and System

1. Multi-Factor Authentication must be used on all applications, systems, programs, web apps, cloud systems, hardware, and software that contains any sensitive data, are used to process county information, stores county data and any other system that ADP deems applicable.
    a. If an application, program, etc. has an option to turn on MFA (sometimes written as 2FA, 2 factor authentication) then it must be turned on and utilized by the administrator of that program.
    b. If an application, program, etc. has the potential to utilize MFA, either by an add-on option, extra work needed, hardware needed, etc. then MFA must be configured and utilized.
        i. Administrators in this category should contact ADP to discuss what is needed for MFA implementation and a plan should be put in place.
    c. If an application, program, etc. does not have an option for MFA:
        i. The administrator should reach out to the manufacturer/developer of the application to verify if it is possible to add MFA or, if not, if they have plans to add MFA in the future.
        ii. The administrator should notify ADP if MFA is not available.
    d. A program may be given an exemption if decided by ADP. Application administrators may contact ADP to request an exemption for a specific application if they believe MFA is not needed.
    e. If an application has multiple options for MFA, the application administrator must contact ADP to determine which option ADP wants utilized.
    f. ADP reserves the right to add or remove acceptable factors of authentication.

Sec. 7.0 Policy Compliance

1. 25-character password length policy effective for all users November 1st, 2022.
2. MFA policy effective for all users March 1st, 2023

3. The Geauga County ADP-DOIT Department of Information Technology will verify compliance to this policy through various methods including but not limited to periodic walk-throughs, video monitoring, business tool reports, and audits.
4. Non-Compliance
    1. Any business unit found to have violated this policy may be subject to delays in service or product release until such a time as compliance is reached.
    2. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should intentionally disregard of this policy and its procedures be observed.

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

Policy on Reporting and Escalating Cybersecurity Incidents

ADP-25-F-005

Classification Level: PUBLIC

Sec. 1.0 – Applicability

This policy applies to all political subdivisions of Geauga County that are under the statutory oversight of the Geauga County Automatic Data Processing (ADP) Board or that have formally opted into ADP Board services pursuant to Ohio Revised Code (ORC) 307.847. This includes county offices as well as any township, municipal corporation, or other local governmental body within Geauga County that utilizes ADP Board IT services. The policy is to be followed in the event of any **"cybersecurity incident"** or **"ransomware incident,"** as defined by ORC 9.64. For purposes of this policy, a *cybersecurity incident* generally means a significant loss of confidentiality, integrity, or availability of an information system or data, a serious disruption to operations or services, or a major unauthorized network intrusion. A *ransomware incident* is a cyber incident in which malware renders systems or data unusable or encrypted and demands a ransom for restoration. All personnel and officials of the above-mentioned entities are required to comply with this notification policy whenever such an incident is suspected or confirmed. This supplemental policy is designed to work in conjunction with the Geauga County Cybersecurity Policy (ADP-25-F-003), and it shall stand alone as an enforceable document outlining incident notification obligations.

Sec. 2.0 – Policy Information

Issued: 09/01/2025
Reviewed: 09/01/2025

Sec. 3.0 – Purpose

The purpose of this policy is to establish a comprehensive and standardized procedure for reporting and escalating cybersecurity incidents and ransomware events within Geauga County's jurisdiction. Prompt and structured notification is critical to ensure that all appropriate parties – from IT responders up through county leadership and state authorities – are aware of incidents in a timely manner. This policy aims to ensure legal compliance with Ohio's cybersecurity incident reporting requirements and to minimize damage from incidents by enabling quick, coordinated response. By clearly defining who must be notified, how, and when, the policy facilitates effective communication during cyber emergencies. It is grounded in recognized best practices (including the Center for Internet Security's guidelines on incident response communications) to ensure that our approach meets industry standards. Ultimately, this notification policy protects the confidentiality, integrity, and availability of government systems and data by enabling swift action and ensuring that no incident goes unreported or unaddressed.

Sec. 4.0 – Authority

This policy is issued under the authority of the Geauga County Automatic Data Processing Board, which oversees county information technology pursuant to ORC 307.84 and expanded authorities under ORC 307.847. The Geauga County Auditor, as Chief Administrator of the ADP Board, is empowered to enforce cybersecurity standards across all participating political subdivisions. This Incident Notification Policy is also enacted in direct response to ORC 9.64, which requires every political subdivision's legislative authority to adopt a cybersecurity program consistent with accepted best practices (e.g. the NIST Cybersecurity Framework and CIS Controls). ORC 9.64 further mandates that certain state officials be notified following any cybersecurity or ransomware incident. Accordingly, the procedures in this policy are designed to ensure full compliance with state law and to align with the Center for Internet Security (CIS) Critical Security Controls (specifically CIS Control 17 on Incident Response Management). In the event of any conflict between this policy and other local directives, the requirements of state law and ADP Board authority shall prevail. All legislative authorities of participating subdivisions have formally agreed to abide by this policy as a condition of receiving ADP Board IT services, making it binding and enforceable across all covered entities.

Sec. 5.0 – Policy and Procedure

The following incident notification procedures are hereby established for all covered entities. These steps must be followed whenever a cybersecurity incident or ransomware incident is discovered or suspected. The goal is to ensure **immediate internal escalation** to the proper authorities, **prompt external reporting** to state agencies as required by law, and thorough **documentation** of the incident. All notifications should be made as expediently as possible, without compromising ongoing incident response actions. Adhering to these procedures will facilitate a rapid and coordinated response, limit the impact of the incident, and fulfill all legal and oversight obligations.

Sec. 5.1 – Internal Incident Escalation and Notification

Immediate Reporting: Any county employee, IT staff member, or official in a participating subdivision who becomes aware of a potential cybersecurity incident (e.g. system breach, malware infection, data loss, or ransomware attack) must **immediately report** it to the Geauga County ADP **Department of Advanced Research and Cybersecurity (DARC)**. DARC is the ADP Board's cybersecurity incident response team, responsible for first-line incident handling. Initial reports should include all available details (what was observed, time of occurrence, affected systems, etc.). There shall be **no delay in reporting**, even if not all information is available, as early notification is crucial.

DARC Team Assessment: Upon notification, the DARC Team will log the incident and conduct a preliminary assessment to confirm whether a cybersecurity incident or ransomware incident is likely occurring. The DARC Team will immediately begin containment, eradication, and recovery actions as appropriate, in accordance with

the County's Incident Response Plan. At the same time, the DARC Team **escalates the incident to management**: the **Deputy Chief Administrator** of the ADP Board (or his/her designee) must be informed as soon as an incident is deemed credible (or immediately if the situation is obviously serious, such as active ransomware). The Deputy Chief Administrator will ensure the **Chief Administrator** (County Auditor) is notified without delay. This internal escalation (DARC to Deputy CA to Chief Admin) should occur **within hours or sooner** of incident discovery, ideally **immediately upon confirmation** of a breach or attack. Rapid escalation up the chain of command ensures that executive leadership is aware and can marshal resources or make critical decisions early.

Executive Notification: The **Chief Administrator** (ADP Board Chief) upon being informed will evaluate the situation in consultation with the DARC Team and Deputy. If the incident is confirmed (or even strongly suspected) to meet the definition of a significant cybersecurity incident or ransomware event, the Chief Administrator must promptly notify the broader leadership and oversight bodies. Specifically, the Chief Administrator (or Deputy on his behalf) will **notify the ADP Board** members about the incident as soon as practicable. This may be done via an emergency communication to all ADP Board members, describing the nature of the incident and immediate actions being taken. In parallel, the Chief Administrator will ensure that the **legislative authority** of the affected political subdivision is formally notified. For county-wide incidents or incidents affecting any county department, this means notifying the Geauga County Board of County Commissioners. For incidents affecting a specific township, municipality, or other subdivision, this means notifying that entity's Board of Township Trustees, City/Village Council, or equivalent governing council. Notification to the legislative authority should be made **as soon as possible** once the incident is confirmed, ideally within 24 hours of discovery. The communication should come from the Chief Administrator or an authorized ADP official and include a summary of what happened, which systems or data are impacted, and what initial response steps are underway. The purpose is to put the elected leadership on formal notice that their entity is experiencing a cyber incident, so that they can mobilize any support needed and fulfill their statutory duties (such as approving any extraordinary actions or preparing to notify state authorities).

Multi-Entity Incidents: In the event that an incident affects systems or data belonging to **multiple political subdivisions**, **all** impacted entities' legislative authorities must be notified. For example, if a county-hosted system serving several townships is breached, both the County Commissioners and each involved Township's Trustees must be informed. The ADP Board will coordinate these notifications to ensure consistency of information. No affected agency or governing body should be left unaware of an incident that impacts them. Broad internal notification of key stakeholders is critical not only for transparency, but also because ORC 9.64 assigns certain responsibilities to those governing authorities following an incident.

Ransomware Considerations: If the incident is a confirmed **ransomware attack**, the legislative authority's involvement is especially critical. Under ORC 9.64(B), a political subdivision is prohibited from paying a ransom or complying with a ransom demand **unless** its legislative authority (e.g. the Board of County Commissioners or City Council) has **formally approved** doing so via a resolution or ordinance explaining why paying the ransom is in the subdivision's best interest. Therefore, in a ransomware scenario, the Chief Administrator's prompt notification to the affected entity's legislative body enables that body to convene quickly and consider any

necessary resolutions. (Note: This policy itself does not advocate for or against paying ransoms; it simply ensures that the legal precondition – legislative approval – can be met by timely involvement of the elected officials.)

In summary, internal escalation proceeds in **stages**: **Employee/IT Staff -> DARC Team -> Deputy Chief Admin -> Chief Admin -> ADP Board -> Affected Legislative Authority.** Each stage must be carried out as swiftly as possible. At no point should an employee or department attempt to contain or hide an incident on their own or delay escalation. Open communication up the chain is mandatory. These internal notifications can be done via phone, secure messaging, and email as appropriate, with high priority. The ADP Board may convene emergency meetings or conference calls if the situation warrants. The legislative authorities, once notified, should designate a point of contact to liaise with the ADP Board and DARC Team for ongoing status updates. This structured escalation process aligns with CIS best practices by ensuring **defined roles and communication channels** are in place before a crisis occurs.

Sec. 5.2 – External Notification Requirements (State Authorities)

Ohio law requires that **state authorities** be notified following any cybersecurity or ransomware incident affecting a political subdivision. This policy mandates full compliance with those requirements as outlined in ORC 9.64(D). In coordination with the affected entity's leadership, the following external notifications **must** be made for every qualifying incident:

- **Executive Director of Homeland Security (Ohio Dept. of Public Safety):** The political subdivision's legislative authority (or a designated official acting on their behalf) shall notify the Executive Director of the Ohio Division of Homeland Security **as soon as possible, but no later than 7 days after discovery of the incident**. The notification must be done in the manner prescribed by the Executive Director. Typically, this will involve submitting an incident report through a state-designated online portal or contacting the state homeland security office directly with details of the event. The ADP Chief Administrator and DARC Team will assist in preparing this notification – providing technical details, timelines, and any required documentation – but the submission should be authorized by the affected entity's executive leadership or legislative authority in accordance with state guidelines. Seven days is the **maximum** allowable window; whenever possible, the notification should be made sooner (e.g., within the first 1–3 days of confirming the incident) to facilitate prompt state-level assistance or guidance.
- **Auditor of State:** The political subdivision's legislative authority (or designee) shall also notify the Ohio Auditor of State **as soon as possible, but no later than 30 days after discovery of the incident**. The Auditor of State may prescribe a specific form or process for this notification (for instance, reporting through the Auditor's fraud or cyber incident reporting system). As with the homeland security notification, the ADP Board staff will support the affected entity in compiling the necessary information for the report. Details typically include the nature of the incident, systems compromised, data potentially accessed or lost, date of occurrence and discovery, and actions taken in response. The notification to the Auditor of State must be completed within **30 calendar days** of discovering the breach or attack. It is

advisable not to wait until the last moment; an initial report can be filed with preliminary information and supplemented later if needed. Timely reporting to the Auditor of State is not only a legal obligation but also can trigger resources for auditing support or inform state oversight to help other jurisdictions.

For clarity, the **responsibility to ensure these state notifications are made lies with the legislative authority of the affected subdivision**, as per ORC 9.64(D). However, the ADP Board acknowledges that local officials may need technical assistance in understanding and fulfilling these requirements. Therefore, **ADP's Chief Administrator (County Auditor)** or Deputy Chief Administrator will work closely with each affected entity to **facilitate and verify** that the 7-day Homeland Security report and the 30-day Auditor of State report are completed on time. The ADP Board will maintain up-to-date **contact information** and reporting templates for the state notifications, in line with CIS Control 17.2 which advises having ready contact info for external reporting of security incidents. If the state prescribes specific forms, ADP will have those forms on file or accessible and will guide the subdivision through their submission. Copies or confirmations of the submissions should be retained in the incident's documentation file (see Sec. 5.3).

In addition to the legally mandated notifications above, the ADP Board or the affected entity may choose to inform other external parties as appropriate: for example, notifying the **Multi-State Information Sharing and Analysis Center (MS-ISAC)** or the state's cybersecurity rapid response team, especially for widespread or critical attacks. **Law enforcement** (such as the FBI cyber crime division or local law enforcement) should be contacted **immediately** in cases of ransomware, data theft, or suspected criminal breaches – this is strongly recommended as a best practice, though not explicitly required by ORC 9.64. The ADP DARC Team will coordinate with law enforcement contacts when incidents involve criminal activity. These additional notifications do not replace or delay the required state notifications; rather, they complement them by leveraging all available resources to respond to the incident.

All external notifications should be handled with appropriate sensitivity and confidentiality. Communications with state and federal authorities must be accurate and truthful, providing a clear picture of the incident. If certain details are unknown at the time of reporting, that should be stated rather than omitted. The ADP Board will ensure that any follow-up information (for example, discovery of additional impact after the initial report) is also communicated to the relevant state contacts. By adhering to these external notification procedures, Geauga County subdivisions will remain in compliance with state law and will contribute to broader statewide cybersecurity awareness and incident response efforts.

Sec. 5.3 – Incident Documentation and Tracking

Accurate documentation of cybersecurity incidents is an integral part of the response process. For every reported incident, the DARC Team will initiate an **Incident Report** and maintain an **incident log** to track the event from discovery to resolution. At a minimum, the following information should be documented:

- Date and time of initial discovery or report of the incident, and how it was detected.

- The individual who reported the incident (if applicable) and the DARC Team member who received the report.
- A description of the incident, including affected systems, networks, or data, and the known scope of impact.
- Immediate actions taken for containment and remediation (e.g. systems isolated, malware removed, passwords reset).
- Timeline of key actions and decisions, including when internal escalations occurred (when Deputy and Chief Admin were notified, when ADP Board and legislative authorities were notified, etc.).
- Details of external notifications: confirmation of when the Executive Director of Homeland Security was notified (date, method, point of contact) and when the Auditor of State was notified, including any reference numbers or acknowledgments received from those offices.
- Any supportive evidence or artifacts, such as copies of ransom notes, screenshots, log excerpts, or alerts, that help describe the incident.
- Final resolution details, including how and when systems were restored to normal operation, and any longer-term corrective measures implemented (patches, changes in configurations, user training, etc.).
- Post-incident analysis notes, including root cause (if identified), and recommendations to prevent similar incidents in the future.

The DARC Team is responsible for keeping the incident log up-to-date throughout the lifecycle of the incident. A unique incident ID shall be assigned for reference. All internal communications and decisions should be timestamped in the record. If the incident spans multiple days or weeks, the log should record daily progress updates. The Deputy Chief Administrator and Chief Administrator will review these logs during and after the incident to ensure thoroughness. Once an incident is closed, a formal **Incident Report** should be compiled by the DARC Team and approved by the Chief Administrator. This report will summarize the incident and include all the key details listed above in a concise format. It serves as the official record of the event.

Storage and Confidentiality: Incident documentation will be stored securely by ADP DARC, with access restricted to authorized personnel (such as the DARC Team, ADP leadership, and auditors as appropriate). Per ORC 9.64(E), records and reports related to cybersecurity incidents and the cybersecurity program are **exempt from public disclosure** and are not considered public records. This means that while incidents must be reported and documented, those records will be kept confidential and will not be released under public records requests. All staff involved in handling incident documentation must ensure the information is protected and shared only on a need-to-know basis. Marking these documents as “Security Incident – Confidential” is recommended. The confidentiality provision encourages honest and complete record-keeping without fear that sensitive security details will be made public.

Incident Tracking System: The ADP Board will maintain an electronic tracking system (which could be part of the helpdesk or ticketing system, or a dedicated incident management system) to log incidents and track their status. Each incident entry should include references to all notifications made and documents collected. The system will also be used to schedule and track the required state notifications (with reminders for the 7-day and 30-day deadlines to ensure none are missed). By tracking incidents in a centralized system, ADP can analyze trends across subdivisions, identify recurring issues, and report summary statistics to oversight bodies (without exposing sensitive details). The ADP Board shall periodically review incident logs to ensure that incidents are being handled and reported in compliance with this policy. Lessons learned from documented incidents will be used to update security measures and to improve this notification policy or the broader incident response plan as needed.

Sec. 5.4 – Notification to Legislative Authorities and Governance Bodies

This policy affirms that **all affected legislative authorities will be promptly notified** in the event of a cybersecurity incident or ransomware incident, as part of the internal escalation process (see Sec. 5.1). The term "legislative authority" refers to the governing body of the political subdivision impacted – for counties, the Board of County Commissioners; for townships, the Board of Township Trustees; for municipalities, the City or Village Council; or any equivalent governing board for other entities. Notification to the legislative authority is a critical step because these bodies have ultimate oversight of their subdivision's operations and bear responsibility for major decisions and statutory compliance in the wake of an incident.

When a legislative authority is notified under this policy, the notification should come from the **Chief Administrator of the ADP Board** or Deputy Chief Administrator, in coordination with the highest administrative officer of the affected subdivision (e.g. a Township Fiscal Officer or City Manager, if applicable). The notification should be made in writing (such as a formal incident briefing memo or email) and, when feasible, also delivered verbally (via phone or in-person briefing) to ensure it is understood. It should clearly state that a cybersecurity incident has occurred, outline known details (without overly technical jargon), and describe immediate steps being taken to address it. The communication must also outline the **obligations of the legislative authority** going forward – for example, reminding them of the required notifications to state agencies (Homeland Security and Auditor of State) within specified timeframes, which the ADP Board will help facilitate, and the restriction on ransom payments without formal approval (if a ransomware event). The legislative body should be advised to convene an emergency or special meeting if needed to discuss the incident, especially if they need to pass any resolution (such as authorizing a ransom payment or emergency expenditures for incident response).

In cases where an incident affects **multiple jurisdictions**, each jurisdiction's legislative authority will be notified as described. ADP will ensure consistent messaging to all parties, while also tailoring the information to each jurisdiction's scope of impact. All such notifications will stress unity and cooperation – for instance, a breach affecting a shared system might require a coordinated response authorized by multiple governing boards. The ADP Board stands ready to brief any legislative body in person if requested, to provide additional context or answer questions about the incident. This open communication with governing authorities aligns with best

practices and legal expectations that those charged with governance are kept informed during significant security events.

Finally, once the immediate crisis phase has passed, the Chief Administrator will provide a follow-up report to the legislative authority summarizing the incident and outcomes. This ensures the governing body has a record for its own oversight purposes and can evaluate any policy or budgetary changes needed. Legislative authorities are encouraged to use the experience as feedback into their cybersecurity programs (as required by ORC 9.64(C)) to continually strengthen defenses. In summary, **no significant cyber incident will ever be concealed from the appropriate governing boards** – transparency and timely notification to leadership is not only a legal mandate but a cornerstone of effective incident response. Each legislative authority, having been duly notified, is expected to fully support and participate in the incident response and recovery efforts within their organization.

Sec. 6.0 – Policy Compliance

DARC Team (Cyber Incident Response Team): The DARC Team is responsible for front-line incident handling and internal escalation. Team members (led by ADP security staff, such as the IT Security Officer or Director of DARC) will receive incident reports, perform initial analysis and triage, and take immediate actions to contain threats. They must promptly inform ADP leadership (Deputy and Chief Administrator) of any verified or suspected major incident. The DARC Team also coordinates technical remediation and provides ongoing updates to management. They maintain the incident documentation (Sec. 5.3) and serve as the liaison to any external technical responders or law enforcement. In essence, DARC is the central hub for managing the incident and ensuring all notification steps are executed – they track that internal notifications up the chain have occurred and assist in preparing information for external notifications. DARC must also maintain current contact lists (on-call rosters, key agency contacts, etc.) so that no time is lost in reaching the right personnel during an emergency.

Deputy Chief Administrator (ADP Board Deputy CA): The Deputy Chief Administrator acts as the intermediary between the technical responders and the executive leadership. When notified of an incident by DARC, the Deputy Chief Administrator verifies that the Chief Administrator is informed immediately. The Deputy may help assess the severity/impact of the incident for the Chief Administrator and coordinate resource needs (e.g. engaging additional IT staff, outside consultants, or notifying county emergency management if needed). He or she may also directly communicate with department heads or local officials of the affected entity to gather or disseminate information. During the incident, the Deputy CA helps manage the flow of information: ensuring the ADP Board members are kept updated, and that the DARC Team receives any guidance or decisions from the Chief Administrator. The Deputy is essentially the incident manager on the administrative side, making sure the policy's steps are followed and that nothing falls through the cracks in the escalation and reporting process.

Chief Administrator (County Auditor, ADP Board Chief): The Chief Administrator has overall authority for incident response and is the primary decision-maker during cybersecurity emergencies. Upon notification of an incident, the Chief Administrator will determine (in consultation with DARC and the Deputy) whether the

incident triggers this notification policy (virtually all but trivial events will). The Chief Administrator ensures that the ADP Board is alerted and convened if necessary. He or she takes charge of communications with the political subdivision's top leadership (e.g. contacting the Commissioners, Trustees, Mayor, or Council President as appropriate). The Chief Administrator authorizes the content of external notifications to state agencies to guarantee accuracy and compliance. This role also entails briefing other key stakeholders (for example, issuing statements to other unaffected departments to raise awareness, or to the media if needed – though media communication is outside the scope of this internal policy, any public messaging would be coordinated by the Chief Administrator with approval of the affected entity's leadership). The Chief Administrator is accountable for ensuring that the requirements of ORC 9.64 are met. Post-incident, the Chief Admin will report to the ADP Board on the incident and may recommend policy or security control changes based on what was learned.

Geauga County ADP Board: The ADP Board provides governance and oversight during cybersecurity incidents. While the Board may not be involved in day-to-day response, it must be **notified** promptly of major incidents (by the Chief Administrator, per this policy) and may be convened in an emergency session if the situation warrants Board-level action. Such actions could include approving emergency funding for incident response, authorizing engagement of external incident response contractors, or coordinating multi-jurisdictional issues. The Board's members, which include elected officials as defined by ORC 307.84/307.847, also serve as liaisons to their respective areas (for example, if a Board member is a county commissioner, they will liaise with the full Board of Commissioners; if a township trustee sits on the ADP Board, they will liaise with their Township, etc.). The ADP Board is responsible for the overall enforcement of this notification policy across all subdivisions. It will review compliance after each incident – for instance, confirming that notifications were made in the proper timeframe – and address any shortcomings. The Board also ensures that this policy remains up-to-date with any changes in state law or best practices (see Sec. 8.0). In short, the ADP Board stands at the top of the escalation pyramid, backing the Chief Administrator in requiring cooperation from all entities and providing the necessary authority to enforce the policy's mandates.

Legislative Authorities of Political Subdivisions: The legislative authority (County Commissioners, Township Trustees, Municipal Councils, etc.) of each covered entity holds ultimate responsibility for that entity's cybersecurity posture under ORC 9.64(C). In the context of incident notification, the legislative authority's role is to receive incident reports from the ADP Board/Chief Administrator and then take required actions. Those actions include ensuring the proper **state notifications** are filed within deadlines (the legislative body will typically delegate the actual task to an official like a City Manager, Township Fiscal Officer, or Administrator, but must oversee that it gets done). If a ransomware incident occurs, the legislative authority must deliberate and decide whether any ransom will be paid; they are the only body that can authorize compliance with a ransom demand, via formal resolution, as noted earlier. Legislative authorities are also expected to support the response effort by allocating necessary resources or emergency funds and by cooperating fully with ADP and law enforcement. Each legislative authority should designate a member or senior staff as a point-of-contact to interface with the ADP Board during incidents. Ultimately, the governing boards are accountable to their constituents and

to the state for how incidents are handled; this policy gives them the framework to meet those obligations through timely notification and action.

Executive Director of Ohio Homeland Security (External): This state official (within the Department of Public Safety's Division of Homeland Security) is the recipient of the 7-day incident notifications under ORC 9.64(D)(1). While not an internal role, it is important to recognize their part in the broader process – upon receiving a report, the Executive Director's office may follow up with the local subdivision or offer incident response assistance from state resources. The ADP Board will maintain open channels with the state homeland security division to facilitate smooth reporting. The Executive Director's prescribed reporting mechanism must be adhered to (for example, an online form or phone hotline).

Auditor of State (External): The Auditor of State's office is the recipient of the 30-day incident notification under ORC 9.64(D)(2). The Auditor's role is primarily oversight; they track incidents across Ohio's local governments and may incorporate the information into audits or security recommendations. After a notification, the Auditor's office might request additional information or even conduct a review of the affected entity's systems (especially if the incident raises concerns of financial fraud or mismanagement). Internally, ADP and the affected subdivision must cooperate with any such follow-up. The Auditor of State also ensures that the reported incidents remain confidential (as they are exempt from public record) and may issue guidance to local governments on improving security post-incident. This policy acknowledges the Auditor's authority and commits Geauga County subdivisions to full compliance with any directives or requests from the Auditor's office in relation to a reported cybersecurity incident.

All Employees and Users: Finally, every user of Geauga County or participating subdivision has a responsibility in incident notification. As stated, users must report signs of cybersecurity incidents immediately to the ADP Service Desk or DARC Team. They should not ignore anomalies (e.g., unusual pop-ups, lost devices, suspected phishing emails that were clicked, etc.). Users are the "eyes and ears" on the ground; prompt reporting can significantly reduce the damage of an incident. This policy makes it clear that there will be no retaliation for reporting a security issue – in fact, it is required. Users must also cooperate with IT and investigators during an incident (providing information, disconnecting devices if told to, etc.). A culture of prompt incident reporting and open communication is essential for this policy to succeed. Each department head is responsible for reinforcing this message to their staff as part of cybersecurity awareness training.

Sec. 7.0 – Policy Compliance and Enforcement

Compliance Monitoring: Compliance with this notification policy will be monitored by the ADP Board and the Departments of DATA and DARC. After any cybersecurity incident, the ADP Chief Administrator will conduct a *post-incident review* to evaluate whether all required notifications (internal and external) were made in accordance with the policy and within mandated timeframes. The incident documentation (Sec. 5.3) will be

examined against the policy's requirements as a checklist. Additionally, periodic drills or tabletop exercises may be conducted to test the incident notification process – for example, simulating a cyber attack to see if the DARC Team and officials follow the escalation steps properly. Results of such tests will be used to improve training and procedures. The ADP Board may ask for regular reports on the status of compliance, such as whether any incidents in the quarter occurred and if so, were they handled per policy. The Ohio Auditor of State's audits may also review whether the subdivision complied with ORC 9.64's notification provisions; a failure to report an incident could result in audit findings or other sanctions. Therefore, compliance with this policy also supports broader regulatory compliance and will be treated as a priority.

Enforcement Measures: All individuals and entities covered by this policy are expected to adhere strictly to its procedures. Non-compliance will be addressed promptly and decisively. Potential enforcement actions include:

- **For Individual Employees or Officials:** Failure to report an incident or attempting to conceal a breach in violation of this policy may lead to disciplinary action, up to and including termination of employment or removal of system access. Similarly, if an employee ignores the escalation protocol (for instance, tries to "handle" a serious incident alone without telling DARC), that is grounds for discipline. Elected officials who do not follow through on their notification duties will be formally reprimanded by the ADP Board and could face public accountability for violating state law.
- **For Departments or Subdivisions:** If a particular department or participating subdivision fails to abide by the notification policy (for example, leadership was informed of an incident but did not notify the ADP Board or delayed the required state reports), the ADP Board may exercise its authority to enforce compliance. This can include issuing a written notice of violation to the governing body, mandating additional cybersecurity training, or temporarily limiting the subdivision's network access if needed to protect the rest of the county infrastructure. In extreme cases, consistent non-compliance could result in the ADP Board reconsidering the provision of IT services to that entity, since such behavior endangers the wider network community.
- **Legal Consequences:** Non-compliance with the state reporting timelines in ORC 9.64(D) could potentially subject the subdivision to state-level consequences. While ORC 9.64 does not specify penalties, failure to report might be noted in Auditor of State reports or could lead to increased scrutiny. Moreover, not involving the legislative authority or paying a ransom without a resolution (ORC 9.64(B)) would be a direct violation of law. This policy's enforcement mechanisms are in place to prevent such legal breaches by ensuring everyone knows and follows the rules.

Positive Enforcement: The ADP Board also encourages a proactive compliance culture. Subdivisions that consistently follow the notification policy and demonstrate a strong incident response posture will be recognized in ADP Board meetings or annual reports. This positive reinforcement underscores that complying is not just about avoiding penalties, but about responsibly safeguarding community resources.

In summary, this policy has the full force of ADP Board authority and relevant law behind it. All personnel and member entities must treat these notification requirements as **mandatory**. The ADP Board will take any steps

necessary to enforce the policy, for the benefit of the entire network of Geauga County governments and the citizens they serve.

Sec. 8.0 – Policy Compliance and Enforcement

This Cybersecurity Incident Notification Policy shall be reviewed on a regular basis (at least annually) by the ADP Board's Chief Administrator in consultation with the DARC Team and legal counsel. Revisions will be made as needed to adapt to new threats, changes in technology, or updates in law and best practices. In particular, any changes to ORC 9.64 or related state cybersecurity requirements will be promptly reflected in this policy. For example, if the state adjusts the notification deadlines or adds additional agencies to notify, this document will be updated to remain in compliance. Revisions may also incorporate lessons learned from actual incidents and exercises – if an after-action report indicates that certain notification steps could be improved or clarified, those changes will be considered.

All revisions to this policy must be approved by the Geauga County ADP Board. Minor administrative updates (such as updating contact information or titles) can be made with approval of the Chief Administrator and then communicated to the Board. Major substantive changes will be presented to the ADP Board in a formal session for review and approval. Once approved, a new issue date and revision number will be assigned, and the policy will be re-published and distributed to all covered entities. All users and officials covered by the policy are expected to familiarize themselves with the latest version. The "Policy Information" section (Sec. 2.0) will log the issue/review dates for transparency.

This policy is a living document. As cybersecurity best practices evolve (guided by organizations like CIS and NIST) and as the county's own capabilities grow, the notification procedures herein will be refined. However, the core principles – prompt internal escalation, timely external reporting, thorough documentation, and leadership awareness – are expected to remain constant. Suggestions for improvement of this policy may be submitted to the ADP Board at any time. The ADP Board is committed to continuously strengthening Geauga County's cyber incident preparedness and will update this policy to ensure it remains an effective tool in that effort.

Effective Date: This policy becomes effective immediately upon issuance. All covered political subdivisions shall acknowledge receipt of this policy and affirm their commitment to comply.

Supplemental to Main Policy: This document is designated as Policy ADP-25-F-005 and serves as a supplement to the Geauga County Cybersecurity Policy ADP-25-F-003. It can be enforced as a standalone policy regarding incident notifications. Any existing incident response or reporting procedures in individual departments or subdivisions should be updated to conform to this county-wide standard. By following this notification policy, Geauga County and its subdivisions will be better equipped to respond to cybersecurity incidents in a unified, compliant, and effective manner.

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

Date	Revision Number	Revision Made By	Revisions
09/01/2025	Initial	Frank Antenucci	Initial Policy Created.

Charles E. Walder, Geauga County Auditor — Date

Automatic Data Processing Board Chief Administrator

Cybersecurity Awareness Training Policy

ADP-25-F-006

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:	06/15/2022
Revised:	08/20/2025
Reviewed:	07/16/2025

Sec. 3.0- Purpose

To establish best practices and requirements for all Geauga County Network users to actively participate in cybersecurity awareness training and simulated email phishing training as well as to set remedial action and procedures for non-compliance.

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.

Sec. 5.0- Policy and Procedure

1. **Cybersecurity Awareness Training**

   ADP provides Cybersecurity Awareness Training for all Geauga County Network users as well as contractors and third-party vendors who access County institutional data or its supporting systems. Provided training(s) will address current cybersecurity concerns, including phishing and social engineering, to keep users updated on the most recent types of attacks and how to spot them. Additionally, ADP conducts monthly simulated phishing

training. ADP and Geauga County leadership fully recognize the time and effort required to complete these trainings, particularly amid the demanding schedules of County personnel. However, the increasing frequency and sophistication of cyber attacks — both nationwide and within Ohio — pose a significant risk to public institutions. Several counties across the state have recently suffered cybersecurity breaches, highlighting the urgent need for robust preventative measures. As public servants, it is our collective duty to protect county resources, funds, and data. To do that, we must be able to quickly identify attacks and know how to report them. Cybersecurity awareness training will help everyone who uses the Geauga County Network achieve this goal and reduce the risk of cyber attack.

2. **User Requirements**
   - **a.** All newly hired employees, new Geauga County Network users, or new vendors or contractors with access to the Geauga County Network are required to complete the ADP assigned New Hire Cybersecurity Awareness Training within 14 days of their start date or prior to receiving access to County IT systems and data.
   - **b.** All Geauga County Network users, including vendors and contractors with access to the Geauga County Network, are required to complete yearly Cybersecurity Awareness Training provided by ADP.
     - i. ADP has partnered with The Ohio Cyber Range Institute (OCRI) to bring the Ohio Persistent Cyber Improvement (OPCI) cybersecurity awareness program to all Geauga County Network users. This program, funded through the State of Ohio and the Cybersecurity and Infrastructure Security Agency (CISA), is no cost to Geauga County.
       1. OPCI training categorizes users into 4 categories:
          a. General Staff, Non-IT
          b. IT/Cybersecurity Professional
          c. IT/Cybersecurity Manager/Executive
          d. Organizational Manager/Executive
       2. All users will be designated into one of these four categories based on their role in the office/agency.
       3. Each category has differing training requirements, including course subject and length, with times ranging from less than 2 hours to an estimated 13 hours, depending on the role.
     - ii. In addition to the OPCI training, ADP will deploy short cybersecurity awareness trainings throughout the year to keep users refreshed on their cybersecurity awareness.
     - iii. ADP will provide clear and timely communication to all users regarding the scheduling of cybersecurity awareness trainings, including notification of training availability and associated completion deadlines. If not completed within the specified time frame, users will be considered out of compliance with this policy. Out of compliance users and their supervisors will be notified via email that they are past due on their training requirement and will be given 7 days to complete the training before their access to the Geauga County Network is disabled, including access to their workstation and email account. If, after 7 days, the user has not completed their past due training, ADP will revoke the user's access. To re-instate a user's access, the user's supervisor must request in writing that ADP re-instate their access and must assure ADP that the user will complete their required training within one week of re-instatement. ADP will verify compliance is met and, if not, will revoke access again and ADP will refer the situation to ADP executive leadership. Repeated non-compliance will be referred to ADP executive leadership.

iv. Cybersecurity awareness trainings outside of the above-mentioned trainings may also be required by ADP and ADP will communicate this to the user group that must take this training, for example: IT personnel. These trainings may have different timelines and requirements than those noted above. Users who do not complete their training in the required timeframe will be subject to having their access revoked after 7 days past due in the same manner as described in 5.2.b.iii.

c. ADP offers in-person cybersecurity awareness training for county agencies, offices, departments, and municipalities at request. If you wish to request in-person cybersecurity awareness training for your employees, please reach out to ADP. Note that this training would be in addition to those mentioned above and would not remove the requirement to take the above training.

d. All Geauga County Network users with email access will be automatically enrolled in monthly simulated phishing training. Users can expect to receive at least one simulated phishing exercise a month. The simulated phishing emails are designed to resemble real phishing emails observed in the Geauga County Network environment and will vary in difficulty, including possibly spoofing real county domains and addresses. Users are tasked with identifying all suspicious emails that arrive in their inbox and instructed to use the Phish Alert Report button in Outlook to report the email. If the Phish Alert Report button is used on the simulated phishing email, the user will be greeted with a "congratulations" pop-up, indicating they have passed the exercise. Those that interact with the simulated phishing email by opening the malicious link or attachment or responding to the sender will receive a notice that they failed the exercise. Those that do not interact with the simulated phishing email, but also do not report it, neither pass nor fail the exercise.

i. ADP may choose to reward those that pass the exercise. An example may be entering those that pass the exercise in a raffle. ADP will announce when rewards will be used and what the reward will be.

ii. Failure of the exercise may result in remedial training for the individual. Repeated failures may result in more intense or longer training or may also result in loss of access to the Geauga County Network.

3. Information Technology Employee and Privileged User Requirements

a. All county employees that are employed by ADP DARC or DATA, are in an Information Technology role or adjacent role, or have a privileged user account, may be required to complete training in addition to those mentioned above.

4. County Designated Cybersecurity Team

a. County employees that are part of ADP DARC or have been designated as part of the core Cybersecurity Team or Incident Response Teams are required to complete the above Cybersecurity Awareness Training required by all county employees mentioned in 5.2.b, as well as the additional annual training required in 5.3.a. Additionally, there will be required more intensive training(s) focusing on Cybersecurity, incident response, and related topics.

5. Responsibility of Directors, Supervisors, and Managers

a. Users who fail to complete the required cybersecurity awareness training by the designated deadline may have their system and email access suspended, which can adversely affect departmental operations. It is the responsibility of management to ensure that all personnel under their supervision complete the assigned ADP security awareness training on time and remain in compliance to avoid disruptions to productivity.

Sec. 6.0 Policy Compliance

A. The Geauga County ADP Department of Information Technology will verify compliance with this policy through various methods including but not limited to periodic walk-throughs, video monitoring, business tool reports, and audits.

B. Non-Compliance

1. Any business unit found to have violated this policy may be subject to delays in service or product release until such a time as all employees in their care have received and completed the appropriate cybersecurity and security awareness training.
2. Users in non-compliance may be subject to removal of access to IT systems including workstations and email.
3. Responsible parties may be subject to disciplinary action by their appointing authority, up to and including termination of employment, should intentional disregard of this policy and its procedures be observed.

_____ _____

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

Date

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

Geauga County Endpoint Quarantine Policy

ADP-25-M-001

Classification Level: CONFIDENTIAL

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: 06/18/2025
Reviewed: 06/18/2025

Sec. 3.0 – Purpose

To define a consistent and rapid process for isolating compromised or high-risk endpoint devices to contain cybersecurity threats and prevent spread within the County network. The policy supports CIS Controls and promotes effective containment, recovery, and compliance with security best practices.

Sec. 4.0 – Authority

This policy is issued by the Geauga County ADP Board. ADP DATA (Department of Advanced Technology and Applications) is responsible for county-wide IT infrastructure, while DARC (Department of Advanced Research and Cybersecurity) has full authority to initiate and manage endpoint quarantine and response efforts. All County offices must adhere to this policy under Ohio Revised Code § 307.847.

Sec. 5.0 – Policy and Procedure

5.1 – Quarantine Triggers

Any County device identified by automated tools (e.g., CrowdStrike, Umbrella, Defender, etc.) or DARC staff as compromised or suspicious must be immediately isolated from the network. Quarantine must happen as quickly as possible, without prior approval. **Endpoint Quarantine Requirement:** Any County-managed endpoint device that is identified by automated security systems or DARC personnel as potentially compromised **must be immediately isolated** from the County network. This full quarantine mandate applies in

all cases where a device is flagged for indicators of compromise, such as active malware infection, unauthorized intrusion, detection of a harmful program (virus, ransomware, spyware, PUP, etc.), or other signs of breach or abnormal behavior. Common detection sources include alerts from endpoint protection platforms (e.g. CrowdStrike Falcon or similar EDR tools), antivirus or intrusion detection systems, threat intelligence feeds, or direct observation by DATA/DARC staff. Upon such an alert or identification, the device in question shall be treated as high risk and removed from network connectivity **without delay**. Prompt containment of affected systems is critical to prevent an initial incident from spreading laterally to other County systems. Accordingly, quarantine actions should be initiated as soon as possible once an alert is received or a compromise is suspected, even if after-hours or on weekends. No prior managerial approval is required to commence isolation of a threatened endpoint; protecting the County's network takes precedence over normal operational considerations in these cases. In alignment with best practices for incident response, responders will "contain first, investigate second," ensuring the threat is halted before it can cause further harm.

5.2 – Isolation Requirements

Quarantined devices must be completely disconnected from internal and external networks, with the exception of secured management access for DARC staff. Network isolation may be implemented automatically or manually. Users must not attempt to bypass isolation.

Network Isolation Procedure: When an endpoint is quarantined under this policy, it shall be completely cut off from all regular network access – both the County internal network and any external Internet connection – except for connectivity specifically needed for remote security remediation. In practical terms, this means the device will be **fully isolated** from other systems, preventing it from communicating with servers, workstations, or external services, thereby halting any ongoing attack or malware propagation. The only network traffic permitted for a quarantined device will be limited to **secure management channels** that allow IT administrators to assess and clean the machine. For example, the endpoint may maintain a connection to the County's endpoint security console or management server so that security teams can run scans, apply patches, or collect forensic data. Aside from such whitelisted management or diagnostic tools, all other network traffic from the device will be blocked. This containment may be achieved by technical means (such as the endpoint protection platform's "network contain" feature that automatically restricts the host's communications) or by manual network controls (such as disabling switch ports, wireless access, or instructing the user to disconnect the device). The isolated device should be physically segregated if needed (for instance, kept powered off or on an unplugged network segment) to ensure it cannot inadvertently reconnect to the enterprise network. During quarantine, users must refrain from using the device altogether until it is cleared – they should not attempt to bypass the isolation (e.g. by connecting to an alternate network or using mobile tethering), as doing so would violate this policy and could worsen the incident. DARC will maintain secure remote access to quarantined hosts via approved tools to facilitate analysis and remediation efforts while the device remains otherwise cut off from County resources

5.3 – DARC Authority

DARC has full discretion to quarantine any County device based on observed threats or alerts. No department, Office, or user is exempt, including critical operations.

5.4 – Investigation and Remediation

Once quarantined, DARC will assess, remediate, and document the issue. Remediation may involve malware removal, patching, reimaging, or other steps. Access credentials may be reset as needed.

Incident Investigation and Remediation: Once an endpoint has been quarantined, the IT Department (led by DARC security analysts and support from system technicians) will conduct a thorough investigation of the device. The goal of this analysis is to determine the nature and extent of the compromise and to eradicate any malicious code or unauthorized access present. Security responders will collect relevant forensic data from the quarantined system (memory dumps, disk images, logs, etc. as needed) to identify malware, indicators of compromise, and affected accounts or data. Standard incident response containment practices will be followed, such as scanning for malware and vulnerabilities, and **capturing forensic images** of the system if required for deeper analysis or evidence preservation. During this phase, the team will also assess whether the incident has spread to other systems; if so, additional devices may be quarantined under this policy to contain the broader threat. Remediation on the quarantined device may include removing or neutralizing malware (through anti-malware tools or manual cleanup), applying security patches to fix exploited vulnerabilities, disabling malicious processes or services, and addressing any security configuration issues that contributed to the incident. In cases of severe compromise, the preferred remedial action may be to **reimage or rebuild** the device from a known-good baseline to ensure all traces of infection are removed. As part of remediation, DARC will also **restrict or reset access credentials** that may have been compromised. User or administrator accounts associated with the breached endpoint could be temporarily disabled, have passwords reset, or be subject to privilege review in order to cut off any stolen credentials the attacker might be using. This aligns with CIS best practices for access control management in an incident: limiting the threat actor's ability to leverage compromised accounts helps contain potential damage. Throughout the investigation and cleanup, DARC staff will keep detailed documentation of findings and actions taken. A summary of the incident (root cause, malware found, data at risk, etc.) will be prepared to inform the clearance decision and any follow-up actions (like user security training or broader infrastructure improvements). The device will remain in quarantine and **not** be returned to normal service until the remediation is verified as successful and the formal clearance process (described below) is completed.

5.5 – Clearance Process

A quarantined device will remain isolated until all of the following approve its release:

1. A certified technician confirms remediation.
2. The Director of DARC approves security compliance.
3. The Deputy Chief Administrator reviews the resolution.
4. The Chief Administrator provides final sign-off.

Quarantine Release and Clearance Process: Removing a device from quarantine and restoring it to the production network shall be done only after a structured **clearance procedure** with documented approvals. The quarantine will **not** be lifted until the device's security status has been validated and the following officials have reviewed and signed off on its return to service: **(1)** a **certified DARC technician** or security analyst who has conducted/verified the remediation steps must certify that the endpoint has been cleaned, patched, and tested and appears fully secure; **(2)** the **Director of DARC** (or their acting designee) must review the incident report and technical certification and approve that all necessary incident response and risk mitigation steps have been taken from a cybersecurity standpoint; **(3)** the **Deputy Chief Administrator** must concur with the assessment and authorize the device's reconnection, ensuring executive oversight; and **(4)** the **Chief Administrator** (County Auditor/ADP Board Chief Administrator) must give final approval to release the device from quarantine. This multi-layer approval process is mandatory for **all** quarantined endpoints, regardless of the device owner's position or the device's function. Its purpose is to ensure that a compromised system is not returned to the network prematurely or without proper scrutiny – a reinstatement of service is effectively treated as a high-risk change that needs thorough vetting. Each approver will sign a clearance form or provide written/email confirmation as evidence of their approval. The forms/approvals will be retained by DARC for compliance records. Only once **all** required signatories have given consent may IT staff reconnect the device to the County network (or remove the network restrictions in the case of a soft quarantine). In coordination with the approvals, any final steps (such as re-enabling network ports or uninstalling quarantine agents) will be carried out and functionality of the device will be verified. The user of the device will be notified when it is cleared for normal use. If any approver is not satisfied that the device is fully secure, they may withhold clearance pending further action (for example, requiring an additional malware scan by an external specialist, or a longer observation period). This ensures that **multiple layers of leadership** agree the risk is addressed before the County accepts the device back into its environment. The clearance process underscores accountability and rigor in restoring quarantined systems to operation.

Approval must be documented and retained. No device may return to the network without completing this process.

5.6 – No Exceptions for Critical Devices

Mission-critical or high-profile devices must follow this policy without exception. These devices may undergo deeper forensic analysis before clearance.

5.7 – Timeliness and Reporting

All incidents must be contained immediately and reported. Users must report suspicious activity, and DARC will document events and notify leadership as needed. Containment, eradication, and lessons-learned will follow the County's incident response framework.

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. The Department of IT may also require users to complete periodic security awareness training related to this policy.

Enforcement: 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. DARC 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.

All users and departments must comply with this policy. ADP DATA and DARC will conduct training and periodic reviews to ensure readiness.

Sec. 7.0 – Policy Revisions

This policy will be reviewed at least annually or as needed to reflect changes in threats, regulations, or CIS Controls. Updates will be documented and communicated accordingly.

Signed by:
Charles Walder
5ECDE9230E05438...

9/12/2025 | 13:01:38 EDT

Charles E. Walder, Geauga County Auditor — Date

Automatic Data Processing Board Chief Administrator