**RESOLUTION ADOPTING THE ASHTABULA COUNTY COMPUTER SYSTEMS USE POLICY, INCLUDING CYBERSECURITY AND ARTIFICIAL INTELLIGENCE PROVISIONS**

WHEREAS, the Ashtabula County Board of Commissioners is responsible for establishing policies governing the use, security, and protection of County-owned computer systems, networks, data, and information technology resources; and

WHEREAS, the Ashtabula County Data Board (ACDB) has developed and updated a comprehensive Computer Systems Use Policy that governs acceptable use, cybersecurity practices, data protection, internet usage, mobile devices, storage of electronic data, and the responsible use of Artificial Intelligence (AI) technologies by County employees, elected officials, contractors, and other authorized users; and

WHEREAS, the Computer Systems Use Policy includes provisions addressing cybersecurity safeguards, user responsibilities, system monitoring, data privacy and security, incident reporting, and compliance with applicable state and federal laws, including Ohio Revised Code Section 9.64, as enacted through House Bill 96; and

WHEREAS, the policy further establishes standards for the authorized and ethical use of Artificial Intelligence tools in County operations, including restrictions on data input, requirements for human oversight, training obligations, and accountability for accuracy, bias, and security; and

WHEREAS, the Board of Commissioners finds that adoption of the Computer Systems Use Policy is necessary to protect County information systems, ensure continuity of operations, mitigate cybersecurity risks, and provide clear guidance to all users of County technology resources;

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF COMMISSIONERS OF ASHTABULA COUNTY, OHIO:

**SECTION 1.**
The Ashtabula County Board of Commissioners hereby adopts the Ashtabula County Data Board Computer Systems Use Policy, dated December 3, 2025, including all sections related to cybersecurity, internet usage, mobile devices, electronic data storage, violations, user responsibilities, and the use of Artificial Intelligence, as the official policy governing the use of County computer systems and information technology resources computer usage policy.

**SECTION 2.**
The Computer Systems Use Policy shall apply to all Ashtabula County employees, elected officials, contractors, interns, temporary staff, and any other individuals authorized to access or use County-owned or County-managed computer systems, networks, devices, or data, as set forth in the policy.

**SECTION 3.**
The County Information Technology Director and the Ashtabula County Data Board, in coordination with the County Administrator and Human Resources, are authorized and directed to implement, administer, enforce, and periodically review the Computer Systems Use Policy, including required training, acknowledgements, and compliance measures.

**SECTION 4.**
All records, documentation, system configurations, logs, and security-related materials associated with the administration of the Computer Systems Use Policy shall be treated as confidential and exempt from public disclosure to the extent permitted by Ohio law, including Ohio Revised Code Section 9.64(E).

**SECTION 5.**
The Board of Commissioners finds and determines that all formal actions taken in adopting this Resolution were conducted in an open meeting of the Board, and that all deliberations leading to such actions were held in compliance with Ohio Revised Code Section 121.22.

**SECTION 6.**
This Resolution shall take effect immediately upon its adoption.

**ASHTABULA COUNTY COMMISSIONERS**

**CERTIFICATION PAGE**

**Resolution No. 2025-562** **December 23, 2025**

**RESOLUTION ADOPTING THE ASHTABULA COUNTY COMPUTER SYSTEMS USE POLICY, INCLUDING CYBERSECURITY AND ARTIFICIAL INTELLIGENCE PROVISIONS**

**Upon the motion of Kathryn L. Whittington, seconded by Casey R. Kozlowski.**

**VOTE:**

| | |
|---|---|
| **J.P. Ducro IV** | **Aye** |
| **Casey R. Kozlowski** | **Aye** |
| **Kathryn L. Whittington** | **Aye** |

**CERTIFICATE OF CLERK**

IT IS HEREBY CERTIFIED that the foregoing is a true and correct transcript of a resolution acted upon and duly passed by the Board of County Commissioners of Ashtabula County, Ohio, on the date noted above.

Lisa Hawkins

Lisa Hawkins, Clerk of the Board
Board of County Commissioners
Ashtabula County, Ohio

Ashtabula

COUNTY, OHIO

*Where great things happen.*

# Policy Manual for ACDB

*(Ashtabula County Data Board)*

# Computer Systems Use

# Contents

Introduction ..... 3

Definitions ..... 3

Disclaimers ..... 4

User Rights and Responsibilities ..... 5

IT Staff Rights and Responsibilities ..... 6

Proper Use ..... 7

Mobile Devices ..... 8

Copyrights and Licenses ..... 9

Internet Usage ..... 9

Use of Artificial Intelligence (AI) ..... 11

Storage of Electronic Data and Documents ..... 14

Violations ..... 14

User Responsibility ..... 15

User Acknowledgement Statement ..... 16

Acknowledgement /Signature Page ..... 17

# Introduction

The policies and guidelines presented here apply to the computer systems of the Ashtabula County Data Board, hereinafter known as "ACDB", regardless of their operating system or manufacturer. It is a privilege that the Ashtabula County Data Board Computer System (ACDBCS) extends to the staff and the public who are trusted to make responsible use of computing resources. If you violate that trust, you may lose that privilege through various processes described in this document. Most of the policies and guidelines presented in this document are expressed in general terms. They are applicable to all facilities and services for which ACDB is providing services. Access to computing resources of ACDB is a privilege, not a right.

# Definitions

- **User:** Any person consuming resources of the ACDB.
- **Authorized user:** Any person whom the ACDBCS authorizes to use facilities that require authorization from the ACDBCS.
- **ACDB:** Refers both to the resources making up the network and the staff members responsible for the operation of those resources.
- **ACDB staff:** Includes a group of full-time or part-time professional staff who work in the areas of hardware and software system support, maintenance, operations, and user support.
- **Internal network:** Network infrastructure that securely connects County-owned equipment such as servers, computers, and printers, and provides internet access to County employees and equipment.
- **External network:** Network infrastructure that is not connected to the internal network and is provided exclusively for connecting to the internet.
- **Artificial Intelligence (AI):** Any system capable of performing tasks that typically require human intelligence, such as learning, reasoning, prediction, or content generation.
- **Generative AI:** AI that produces text, images, code, or other content based on input prompts.
- **Automated Decision System (ADS):** A system that makes or assists in making decisions that can affect individuals or services.
- **Sensitive Information:** Any data classified as confidential, restricted, or personally identifiable (PII).

# Disclaimers

The ACDB allows for computing facilities consisting of hardware, software, and documentation to be available to staff, other offices (inside and outside the Courthouse building), and the public. The use and operation of these facilities are subject to the following disclaimers.

Every effort is made by ACDB staff to prevent loss of data either by human error, hardware or software failure. This is done by making regular backup copies of data stored on equipment under the oversight of the ACDB staff. It must be recognized, however, that in rare cases it may not be possible to restore the latest version of every data file from these backups, and some data loss may occur. Because these cases are outside the ACDB staff's control, the staff cannot be held liable for any loss of data arising directly or indirectly from hardware, software, or human error.

Because the goals of the ACDB are primarily clerical in nature, and the computer systems are generally open to perusal and investigation by users, the security controls may be more restrictive than they would be in other environments. Although an appropriate effort is made to maintain system security, unauthorized access to information may be possible through malicious mischief. The ACDB staff cannot guarantee against loss of privacy, theft of information, damage, or loss of data arising directly or indirectly from the absence or failure of system security protection mechanisms.

Most of the software used on the ACDB equipment is purchased or licensed from third-party vendors, usually without source code. This limits the ACDB staff's ability to repair bugs in this software or to modify the software. If possible, the ACDB staff will make every effort to correct any problems. However, the ACDB makes no warranty, expressed or implied, regarding the computing services offered or their fitness for any particular purpose.

# User Rights and Responsibilities

1. Only properly authorized persons may access ACDB facilities. Proper authorization is provided by ACDB office holders or their delegates through an account issued in the name of the authorized person.
2. An authorized user may not permit other persons (including other authorized users) access through his or her account.
3. To enable the ACDB staff to accurately maintain information about the user of each account, each office holder or their delegate is responsible for supplying current information to the appropriate ACDB staff member, including affiliation and the position held.
4. Providing false or misleading information for the purpose of obtaining access to ACDB facilities is a violation of the Ohio Revised Code Section 2921.13 (A)(5).
5. Each user is responsible for all activities initiated in or on ACDB facilities by his or her account.
6. Users are responsible for selecting a secure password for their account and for keeping that password secure at all times. Passwords should not be written down, stored online, or given to others. Passwords should only be given out to ACDB staff.
7. Users are urged to report any system security violation or suspected system security violation to the ACDB staff.
8. Most ACDB facilities are made available on an unmonitored basis. It is the responsibility of every user to act in such a manner as not to cause damage to the physical equipment. Any type of damage or malfunction should be reported immediately to the ACDB staff so that appropriate action can be taken.
9. Users who borrow hardware, software, or documentation from ACDB are responsible for its proper care and for returning it in a timely fashion.
10. Users are responsible for adhering to all official notices posted in their respective offices. Above all, ACDB users are responsible for using ACDB equipment and software in a manner that is ethical, legal, and not to the detriment of other users or equipment.

# IT Staff Rights and Responsibilities

The ACDB staff generally may do whatever is necessary to carry out its responsibility to maintain the effective operation of the ACDB facilities. The ACDB staff is currently under the oversight of an Information Technology Department Director and the Ashtabula County Auditor.

1. The ACDB staff has the responsibility to make every reasonable effort to maintain the privacy of users' files, electronic mail, and printer listings.
2. ACDB staff have the responsibility to comply with all guidelines of this policy in using and holding personal users' data.
3. In the normal course of examining and repairing system problems, and when investigating instances of improper use of ACDB facilities, the ACDB staff has the right to examine users' files, email, and printer listings, and will maintain the confidentiality of these documents as necessary.
4. When investigations discover improper use, the ACDB staff has the right to: limit the access of those found using facilities or services improperly, disclose information found during the investigation to the office holder and/or law enforcement authorities, and initiate disciplinary actions as prescribed by the office holder's policies and procedures.
5. To protect against hardware and software failures, a backup of all data stored on ACDB servers is made regularly. The ACDB staff has the right to examine the contents of these backups to get sufficient information to diagnose and correct problems with system equipment or software, or to investigate instances of improper use of ACDB facilities.
6. The ACDB staff has the right to monitor all aspects of a system, to determine if a user is acting in violation of the guidelines outlined in this document, with written consent from the elected official.
7. It is the responsibility of the ACDB staff to keep the database of user accounts in the computer system up-to-date. The elected official or office manager is to notify ACDB staff to delete or deactivate the user account and data files once the user is not an employee of one of the respective offices serviced by the ACDB. ACDB staff reserves the right to delete or deactivate user accounts and data files during diagnosis of a problem or regular maintenance.
8. The ACDB staff has the responsibility to provide advance notice of system shutdowns for maintenance, upgrades, or changes so that users may plan around periods of system unavailability. However, in the event of an emergency, the ACDB staff may shut down a system with little or no advance notification. Every effort will be made to give users a chance to save their work before the system is taken out of service.
9. ACDB staff members have the responsibility to report any violations of this policy or state law to the office holder.
10. The ACDB staff may refuse or restrict access to ACDB facilities to any person who has violated the guidelines of this document or who has violated the guidelines of other computer facilities belonging to Ashtabula County.

# Proper Use

The ACDB facilities are provided for use by staff to perform routine work-related assignments. It is also provided to the public for inquiry purposes. All staff and the public are responsible for using these facilities in an effective, ethical, and lawful manner.

1. Staff and public users shall not connect their personal devices to the internal network without written approval from ACDB staff.
2. Staff and public users may connect personal devices to the external network at the discretion of the ACDB.
3. The County shall not be held responsible for any damages, electrical or other, to personal equipment when using courthouse electrical outlets.
4. All users share many resources, such as network bandwidth, disk space, CPU cycles, printer queues, batch queues, login sessions, and software licenses. No user may monopolize these resources. Users should consume as little disk space as possible.
5. ACDB facilities are provided for governmental use and some administrative uses. ACDB facilities shall not be used for commercial or personal gains without the explicit approval of the office holder for which the employee is employed and the ACDB Information Technology Director.
6. Users shall not install, develop, or use programs that harass other users of the system.
   - 6.1. Users shall not install, develop, or use programs that attempt to bypass system security mechanisms, steal passwords or data, or "crack" passwords.
   - 6.2. Users shall not install, develop, or use programs that, by design, attempt to consume all of an available system resource (CPU, memory, swap space, disk space, network bandwidth, etc.).
   - 6.3. Users shall not install, develop, or use programs designed to replicate themselves or attach themselves to other programs, commonly called worms or viruses, malware.
   - 6.4. Users shall not install, develop, or use programs designed to evade software licensing or copying restrictions.
7. Files used or owned by individual users but stored on County equipment should be considered County property, whether or not they are accessible by other users.
   - 7.1. Just as an unlocked door or window does not implicitly grant permission to strangers to enter your house, the ability to read another user's files does not implicitly grant permission to read those files.
   - 7.2. Under no circumstances may a user alter a file(s) that does not belong to him or her without prior permission of the file's owner. The ability to alter another user's files does not implicitly grant permission to alter those files.
8. Because this is a government agency, computer systems are generally open to perusal and investigation by users. This access must not be abused by attempting to harm the systems. Deliberate alteration of system files is vandalism or malicious destruction of governmental property and is subject to prosecution under the Ohio Revised Code.
9. Communications on ACDB equipment may not contain content that a reasonable person would consider to be defamatory, offensive, harassing, disruptive, or derogatory, including but not limited to sexual comments or images, racial or ethnic slurs, or other comments or

images that would offend someone based on race, gender, national origin, sexual orientation, religion, political beliefs, or disability.

10. The system shall not be used to process or send harassing, defamatory, pornographic, or any other illegal materials, and such materials may not be accessed or sent by use of any media contained on any system equipment, computer, or any other media by use of county property.
11. ACDB facilities and network connections may not be used for the purposes of making unauthorized connections to, breaking into, or adversely affecting the performance of other systems on the network, whether these systems are county-owned or not. The ability to connect to other systems via the network does not imply the right to make use of or even connect to these systems unless properly authorized by the owners of those systems.
12. Other organizations operating computing and network facilities that are reachable via ACDB equipment may have their own policies governing the use of those resources. When accessing remote resources from ACDBCS facilities, users are responsible for adhering to both the guidelines outlined in this document and the policies of the other organizations as they pertain. In the event of conflicting policies, this policy will supersede all others.

# Mobile Devices

Definition: A mobile device has an operating system and can run various types of software applications. It can connect to available network systems as well as the internet, be used to read, store, and edit data, and is used for communication.

Mobile devices must be appropriately secured to:

1. Prevent sensitive or confidential data from being lost or compromised
2. Reduce the risk of propagating viruses and other forms of malware
3. Mitigate other forms of abuse of the company's computing and information infrastructure

No personally owned mobile devices are currently allowed to connect with ACDBCS equipment. An exception is allowed for email only and must first be approved by the office holder and ACDB staff before they are permitted access.

Approved mobile devices must contain approved antivirus software verified by the ACDB staff before connecting to the ACDBCS network infrastructure, systems, and/or data. Mobile devices must first be scanned with the approved antivirus software before their first connection to our network infrastructure. It is the owner's responsibility to keep their security software properly updated. If personally owned equipment is not properly updated, it will be removed from access to County resources.

Mobile devices, regardless of ownership, that are not authorized by the ACDB staff are prohibited from connecting to the ACDB infrastructure and/or its resources and must not store, contain, or transmit ACDBCS data.

# Copyrights and Licenses

Copyrights and patent laws protect the interests of authors, inventors, and software developers in their products. The software used on ACDB facilities is operated under license agreements with software suppliers.

1. Software license agreements serve to increase compliance with copyright and patent laws. It is against United States copyright laws and ACDB policy to violate the copyrights or patents on computer software. It is against ACDBCS policy and may be a violation of United States copyright laws to violate software license agreements.
2. Source code for licensed software is not allowed to be included in software that is released for use outside the ACDBCS.
3. The following are considered theft:
   3.1 Making a copy of software having a restricted-use license.
   3.2 Altering system settings to "beat" the license.
   3.3 Possession of volume license keys not obtained legally.
4. Under no circumstances shall any unlicensed software be installed on any system owned by ACDBCS. Any software that is to be installed will be under the direction of ACDB staff.

   4.1. "Unlicensed" means any software program that is not licensed for use by ACDBCS

   4.2. In addition, no portable media that contains personal files shall be loaded onto any system or computer unless authorized by the office holder and ACDB staff.

# Internet Usage

**Scope of Policy**

This document sets forth the policies of the ACDB regarding the use of its computer system (which includes, but is not limited to, email, computers, and related equipment) and the Internet (whether it be an account issued to the employee or the employee's use of his or her personal account on county property).

All employees who use ACDBCS agree by such use to comply with these policies. The ACDB reserves the right to change this policy at any time.

1. **Ownership of Messages**
   ACDBCS and all information stored in them are the property of the County. All information and messages, whether personal or county-related, that are created, sent, received, accessed, or stored on these systems constitute County property.
2. **Business Use**
   ACDBCS resources are provided at county expense and are to be used to conduct County business, but

   2.1. ACDBCS does allow personal use of the Internet under certain conditions. The activity must be done on personal, not county, time.

   2.2. Employees may not use the Internet for streaming audio and/or video. (Example: music, movies, clips, etc.) unless required in the course of their job and authorized by the office holder.

2.3. Employees may not use ACDBCS to view or interact with social networking websites (Example: Facebook, Twitter, etc.) unless required in the course of their job and authorized by the office holder.

2.4. Employees may not use ACDBCS for the creation or distribution of chain letters/emails or passing off the employee's views as representing those of the county.

2.5. Employees may not use ACDBCS for jokes, political causes or activities; football pools, baby pools, or other sorts of gambling; religious activities; list servers for non-work-related purposes; solicitations or advertisements for non-county purposes, including charitable activities.

2.6. ACDB staff reserves the right to immediately suspend internet use if any threats to the ACDBCS equipment or network are found.

3. **No Presumption of Privacy**
Communications on ACDBCS are not private, and security is not guaranteed. Passwords and user IDs are designed to protect county confidential information from outside parties, not to provide employees with personal privacy in the messages.

3.1. In surfing the Internet, employees should remember that all connections and sites may be monitored and recorded by the ACDB staff.

3.2. To ensure the ACDB continues to have access to information on the ACDBCS, employees may not use personal hardware or software to encrypt any email, voice mail, or other information contained in or transmitted by ACDBCS, absent prior written consent from the office holder that employs the employee and the ACDB staff.

4. **Prohibited Activities**
Employees may not use ACDBCS to: upload, download, or otherwise transmit copyrighted, trademarked, or patented material; trade secrets; or other confidential, private, or proprietary information or materials without the consent of the office holder, which employs the employee, and the ACDB staff.

5. **Violations**
Violations of this policy, including breaches of confidentiality or security, may result in suspension of Internet service to the user's account, computer, and/or use of email privileges, or other disciplinary actions, including termination. Employees may be held personally liable for any violation of this policy that results in monetary loss to the county, including costs to correct any violation.

6. **Viruses and Tampering**
Any files downloaded from the Internet and any computer discs received from non-county sources must be scanned for viruses. The introduction of viruses, attempts to breach system security, or other malicious tampering with ACDBCS are expressly prohibited. Employees must immediately report any viruses, tampering, or other system breaches to the ACDB staff.

# Use of Artificial Intelligence (AI)

## Scope of Policy

This policy applies to:

- All Ashtabula County employees, elected officials, contractors, interns, and temporary staff.
- All county departments, offices, and agencies utilizing or interacting with AI tools, including generative AI (e.g., ChatGPT, Copilot, Gemini, Claude), machine learning systems, or automated decision-making platforms.
- All county-owned and third-party AI systems accessed through county devices or networks.

## Policy Statement

Ashtabula County supports the responsible and transparent use of AI to improve efficiency, decision-making, and public service delivery. However, misuse or negligent application of AI may result in data exposure, misinformation, bias, or reputational harm. Employees must use AI tools only for legitimate county business and in compliance with this policy.

## Authorized Use

1. **AI use must support legitimate county operations.**
   Employees may use AI to draft documents, summarize information, generate ideas, or assist with data analysis, provided the use complies with confidentiality and data protection requirements.
2. **Employees must not use personal AI accounts, email addresses, or logins for county business**.
   All AI use related to county work must occur through approved, county-issued accounts and devices. Any AI activity performed under a personal account for county work is a **violation of this policy**.
3. **AI must not replace professional judgment.**
   AI outputs are advisory tools and must always be reviewed and validated by a qualified human employee.
4. **Data input restrictions:**
   Employees must not input any of the following into public AI tools:

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Criminal Justice Information (CJI)
- Financial records, payroll data, or confidential county documents
- Internal credentials, passwords, or proprietary source code

5. **Procurement and deployment**:
Any AI application used for county operations must be reviewed and approved by the IT Department for security, compliance, and ethical alignment.

## Employee Responsibilities

Employees are responsible for:

- Understanding the limitations and potential biases of AI tools.
- Fact-checking and verifying all AI-generated content before use or publication.
- Reporting any suspected misuse, breach, or AI-related incident to the IT or Department Head immediately.
- Following all department-specific data classification and cybersecurity policies.
- Completing all required annual AI awareness and ethics training as mandated by the County IT Department and Human Resources.

## Prohibited Use

***Employees are strictly prohibited from:***

- Using AI to create or spread misinformation, offensive, or discriminatory content.
- Using AI for personal gain, political activity, or outside employment.
- Circumventing county security systems or accessing restricted data.
- Using AI to make final decisions in personnel, legal, or disciplinary matters.
- Using AI to impersonate individuals or departments without authorization.
- Uploading confidential or internal documents to unapproved or public AI services.
- Using personal AI accounts or platforms to perform county business, or using county AI accounts for personal or non-work-related activities.

## Data Privacy and Security

- All AI interactions must comply with county cybersecurity standards and applicable state and federal laws (e.g., HIPAA, FERPA, CJIS, GDPR equivalents).
- AI vendors must undergo a data security review, including assessment of data retention, model training, and storage practices.
- The county reserves the right to log, audit, and monitor AI use across all systems.

## Accuracy, Bias, and Accountability

- Employees must recognize that AI outputs may include factual inaccuracies or implicit biases.
- Departments using AI for analysis, decision-making, or communication are accountable for verifying output accuracy and fairness.
- Any discovered bias or error in AI output must be reported to the IT Department and/or the Department Head

## Governance and Oversight

- ACDB may audit AI usage logs for compliance.
- ACDB will maintain an approved list of AI tools.

## Reporting

- All AI-related incidents or misuse must be reported to IT, HR, or a Department Head immediately.

# Storage of Electronic Data and Documents

### Scope of Policy

This policy applies to:

- All Ashtabula County employees, elected officials, contractors, interns, and temporary staff.
- All county departments, offices, and agencies storing electronic data and documents.

### Storage Location

All electronic data and documents (going forward referred to as "data") must reside on servers managed by the ACDB, with the following exceptions:

1. **3rd Party Contractors**
   Data can be stored in a cloud-based environment, provided it is part of a contract with a 3rd party vendor.

2. **Administered by ACDB Staff**
   If there is a need to store data outside the County network and it is not part of a contract, access accounts must be administered by ACDB staff, and there must be at least 2 ACDB staff members with administrative access.

# Violations

1. The offending employee may be notified and be requested to discuss, in person, with his or her supervisor and the ACDB staff, the violation of policies and procedures. The proceedings may be documented.
2. Any disciplinary action to be taken will be at the direction of the office holder.
3. If the activity is suspected of being a violation of criminal law, ACDB staff shall report this to the County Prosecutor.

# User Responsibility

Account Passwords and Access:

**Windows**
The password on each Windows account expires every 1 year or at the discretion of the Information Technology Director. Approximately one (1) week before the expiration date of your password, the system will notify you of the date that the password is set to expire. If the password has not been modified by that date, the system will allow you to log into your account with the old password one time and prompt you to enter a new password and/or lock you out of your mapped drives (network shares). You will not be able to access your account until the password is modified.

Passwords are to be at least fifteen (15) characters in length and must include at least one of each of upper case letters, lower case letters, numbers, and special characters such as $ or !. Passwords should not be common words that are found in the dictionary or easily guessable (spouse or child names, hobbies, nicknames, pet names, etc.). Passwords are case-sensitive. Passwords may be modified by the user at any time during the 1 year.

Do not share your password with anyone other than the ACDB staff. If you believe someone else may know your password, change your password immediately. If there are more than seven (5) attempts to log on to your system, the network will not let you access that computer. Your account has been locked and can only be unlocked by ACDB staff.

Users should not leave PC's logged into their account unattended. If you leave your desk for any lengthy period of time, you should lock your computer (CTL+ALT+DEL then click on the "lock") or Windows key + L, to ensure that others cannot access your account in your absence. Users should shut down their PC's at the end of their work week.

**Email**
The password for the court's users and some smartphone users' email addresses does not expire. You are required to change your default/initial password. Email accounts are county property. Please treat them as such. Do not click on links or attachments from unknown sources because this is the most common source of infection in systems with computer viruses. Report suspicious emails to the ACDB staff. Emails cannot exceed 30 MB when sending attachments. ZIP files cannot be sent or received, and no warning will be given to the user about this fact. They will be automatically deleted from the system.

# User Acknowledgement Statement

**Purpose:**
The purpose of the "User Acknowledgment Statement" is to educate each user as to his or her Responsibility for safeguarding the ACDBCS resources.

**Policy Statement:**
The Ashtabula County Data Board has implemented a computer system security policy to protect the Ashtabula County Data Board's Computer System resources. The goal of the policy is:

1. To assure that sensitive data is read only by authorized individuals, and is not disclosed to unauthorized individuals or to the public;

2. To protect data and software from improper modification and tampering; and

3. To ensure that the ACDBCS systems, networks, programs, and data are available and accessible when authorized users need them.

4. ACDBCS and all information stored in them are the property of the County. All information and messages, whether personal or county-related, that are created, sent, received, accessed, or stored on these systems constitute County property.

## Acknowledgement

I ACKNOWLEDGE THAT I HAVE RECEIVED A COPY OF THE ACDBCS COMPUTER POLICY MANUAL AND THE ACDBCS SECURITY POLICY USER ACKNOWLEDGMENT STATEMENT. I HAVE READ THE POLICIES, GUIDELINES, AND RESPONSIBILITIES AND UNDERSTAND THE CONTENTS.

**Employee Name (please print)** **Department**

**Employee Signature** **Date**

(This page of the computer use policy form must be returned to ACDB staff. After signing/dating, please give this page to the office holder who employs you and keep the policy for personal reference.)