CULLMAN COUNTY COMMISSION

Cybersecurity Manual

Effective: May 17, 2023 (Approved as part of the Cullman County Employee Handbook)

THIS CYBERSECURITY MANUAL CONTAINS CULLMAN COUNTY'S POLICIES AND PROCEDURES DEALING WITH DATA AND CYBERSECURITY, SOCIAL MEDIA, AND DATA BREACH NOTIFICATION. THESE POLICIES ARE A PART OF THE CULLMAN COUNTY COMMISSION EMPLOYEE HANDBOOK AND ARE INCLUDED IN THAT DOCUMENT.

I-H(A). Data and Cybersecurity Policy and Procedure

As counties rely more heavily on technology to acquire, access, utilize, process, distribute, transmit, store, protect, manage, maintain, dispose of or otherwise handle or communicate information, the county becomes more vulnerable to data and cybersecurity breaches. Human errors, hijacker attacks, and system malfunctions could cause operational disruption, financial impact, and reputational damage to the county. In order to provide guidelines for acceptable and reasonable practices, policies, and procedures that preserve the integrity of and minimize the vulnerability of county data, computer equipment, applications, systems, networks, media storage, and other technology infrastructure (collectively "Data Assets") from illegal or damaging attacks, either knowingly or unknowingly, the Cullman County Commission hereby establishes this Data and Cybersecurity Policy.

The purpose of this policy is to (a) protect the county Data Assets, (b) define the rules for county and personal use of the Data Assets, (c) outline the protocols and guidelines that govern data security measures, (d) provide for the retention and disposal of Data Assets, and (e) list the county's disciplinary process for policy violations.

This policy applies to all county commission offices and departments, including but not limited to, the Sheriff's office, the Revenue Commissioner's office, the probate office, and any other county-funded entity or program, and applies to permanent and part-time employees, remote workers, third-party agents, contractors, consultants, volunteers, suppliers, interns, and any other individuals who have permanent or temporary access to the county's Data Assets (collectively "Users"). This policy applies to all Data Assets and technology infrastructure, whether owned or leased by the county, and to personally-owned devices connected by wire or wireless service to the county network. This policy also applies to Data Assets purchased using any officials' discretionary funds.

1. **Compliance and Training.** Alabama governmental entities, including counties, must comply with the Alabama Data Breach Notification Act of 2018, codified in Ala. Code § 8-38-1 et seq. The Act requires the implementation and maintenance of reasonable security measures for data. Reasonable security measures under the Act include:

   (a) Designation of employee(s) to coordinate the county's security measures to protect against a breach of security;
   (b) Identification of internal and external risks of a breach of security;
   (c) Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards;
   (d) Retention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information;
   (e) Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information; and,
   (f) Keeping the county commission appropriately informed of the overall status of its security measures.

   The Act also requires security evaluation and assessment. Assessment under the Act includes consideration of: (1) the size of the county, (2) the amount and type of sensitive information in the county's possession and, (3) the cost that would be incurred to establish and maintain security measures.

   Non-compliance with this policy may pose risks to the county and to Users, individually. County employees should be trained on cybersecurity measures and this policy within 30 days of employment.

2. **Acceptable Use.** Data Assets are the property of the county. These assets are to be used for business purposes in serving the interests of the county, the residents of the county, and its clients and customers in the course of normal operations. Users are responsible for exercising good judgment regarding the reasonableness of personal

use. Users shall not use the Data Assets or any other means of communication or equipment to engage in activities that are in violation of any federal or state law, or that are in violation of any county policy.

3. **Data Classification.** Users are required to preserve the sanctity of data collected, generated, accessed, transmitted, and stored on the county's Data Assets. Data classification enables the use of data so that information will be protected from unauthorized disclosure, use or modification, and deletion. All data and information entrusted to the county and from third parties falls into one of three sensitivity classifications.

For the purposes of this policy, "sensitive information" is the same as sensitive personally identifying information (SPII) as defined in Ala. Code § 8-38-2(6). Sensitive information is information whose unauthorized disclosure, compromise, or destruction would result in severe damage to the county, its residents, or employees. Users are required to preserve sensitive information. Sensitive information is an Alabama resident's first name or first initial and last name, in combination with any one of the following:

(a) A Social Security number or tax identification number;
(b) A driver's license number or any other unique, government-issued identification number used to verify identity;
(c) Any financial account number in combination with access information (e.g., a security code, expiration date, or PIN);
(d) Any information regarding a person's medical, mental or physical history, condition or treatment;
(e) A person's health insurance policy number or subscriber identification number and unique identifier; or,
(f) A username or email address, in combination with a password or security question and answer.

Restricted information is internal use information that must be guarded due to custody, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal mandates, unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of information could cause monetary loss, damage to the county's reputation, or violate an individual's privacy rights (e.g., educational records, employment history, and biographical information).

Public information is information that is not publicly disseminated, but accessible to the public. This data is either explicitly defined as public information (e.g., employee salary ranges), intended to be readily available to individuals both on and off premises (e.g., an employee's work email address), or not specifically classified elsewhere as protected information. Publicly available information may be subject to appropriate review or disclosure procedures to mitigate potential risks of inappropriate disclosure of data or to organize it according to its risk of loss or harm from disclosure.

Examples of sensitive, restricted, and public information are not intended to be all-inclusive. Additional types of data or information may fall under one of these classifications.

4. **County and Personal Device Security.** When Users use county or personal devices to access information from the county Data Assets, they introduce security risks to county data. A device means, but is not limited to, a laptop, tablet, personal computer, workstation, smart phone or mobile device.

To ensure the security of all county-issued devices and Data Assets, all Users are required to:

(a) Keep all county-issued devices password protected*;
(b) Ensure devices are not exposed or left unattended;
(c) Refrain from sharing private passwords with coworkers, personal acquaintances, or others;
(d) Ensure devices are current with security patches and updates and regularly updated with the latest anti-virus, anti-malware, or security software*;
(e) Install security updates of browsers and systems monthly or as soon as updates are available*;
(f) Discourage use of others' devices to access the county's systems, networks, and technology infrastructure;
(g) Avoid lending county devices to other individuals; and

(h) Use only secure and private networks to log into county systems, networks, and technology infrastructure.

(*NOTE: Some of these functions may be handled directly by the County IT Department rather than the User)

A personal device means, but is not limited to, a laptop, tablet, personal computer, workstation, smart phone, mobile device, or other device that is authorized to access the county's Data Assets or is used to backup any such device and is owned by a User and acquired voluntarily, without payment by the county and without any expectation of reimbursement for any costs related to the purchase, activation, operational/connectivity charges, service or repairs, or other costs that may be incurred related to the device or its use. The county recognizes that Users may use personal devices to access the county's Data Assets. In such cases, Users must report this information to the County Administrator, IT Manager, or designee for record-keeping purposes. To ensure the county Data Assets are protected, all Users are required to:

(a) Ensure all personal devices used to access county-related Data Assets are password protected;
(b) Lock all devices if unattended;
(c) Ensure all devices are protected at all times;
(d) Install and regularly update security patches, anti-virus, anti-malware, and security software; and
(e) Use only secure and private networks.

Devices must be kept up to date with manufacturer or network provided patches. The most recent security patches must be installed on the Data Assets and devices as soon as practical, the only exception being when immediate application would interfere with county operations. At a minimum, patches should be checked for weekly and applied at least once a month.

5. **Email Security**. Protecting email systems internally and externally is a high priority as emails can lead to data theft, corruption, virus infections, phishing attacks, and scams. Therefore, the county instructs all Users to:

(a) Verify the legitimacy of each email, including the email address and sender name;
(b) Avoid opening suspicious emails, attachments, and links;
(c) Be suspicious of phishing, clickbait titles and links (e.g., offering prizes, advice);
(d) Look for inconsistencies or giveaways (e.g., grammatical errors, capital letters, overuse of punctuation marks);
(e) Delete immediately unsolicited email (spam) from unknown parties; and
(f) Refrain from using county email for personal use.

Users should contact the County Administrator, IT Manager, or designee regarding any suspicious emails.

6. **Password Management and Security.** Password leaks can compromise the county's Data Assets. Passwords should remain secret and secure so they will not be easily hacked. For this reason, the county advises all Users to:

(a) Avoid passwords that can easily be guessed (e.g., birthdays);
(b) Remember passwords instead of writing them down. If required to write them down, all Users should keep the paper or digital document confidential.
(c) Exchange credentials only when absolutely necessary. When exchanging in person is impossible, all Users should exchange passwords over the telephone instead of via email, and only if they recognize the individual to whom they are speaking; and
(d) Change passwords regularly.

7. **Clear Desk and Screen Security.** Users must have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk, workstation, or screen and have knowledge of how to protect them. This ensures that all sensitive information, whether it be on paper, a storage device, or a hardware device is properly locked away or disposed of when a workstation is not in use. This will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business. For a clear desk, Users should operate as follows:

(a) When leaving a desk for a short period of time, Users must ensure printed matter containing information that is sensitive or confidential is not left in view.
(b) When leaving a desk for a longer period of time or overnight, Users must ensure printed matter containing sensitive or confidential information is securely locked away.
(c) Whiteboards and flipcharts must be wiped and removed of all sensitive information.

For a clear screen, Users should operate as follows:

(d) When leaving the workstation for any period of time, Users must ensure they lock their computer session to prevent unauthorized access to the network and stored information.
(e) All users must ensure their screens cannot be overlooked by members of the public, or people without the necessary authority when sensitive or confidential data or information is displayed. Where appropriate, privacy filters should be used to protect the information.
(f) Following up to a maximum of 15 minutes of inactivity, the session will be automatically locked as a failsafe measure.

8. **Secure Data Transfer.** Transferring data exposes the county to security risks and requires strict safeguards. Users must:
   (a) Avoid transferring sensitive information to other devices or accounts if at all possible;
   (b) Share sensitive information over the county network and not over public Wi-Fi or a private connection;
   (c) Ensure that recipients of the information are properly authorized and have adequate security measures; and
   (d) Report scams, suspicious emails, privacy breaches, and hacking attempts.

9. **Remote Access.** Users sometimes access the county's Data Assets from a distance. Secure remote access must be strictly controlled with encryption (e.g., Virtual Private Networks (VPNs)) and strong passwords. It is the responsibility of Users with remote access privileges to the county's network to ensure that their remote access connection is given the same consideration as the User's on-site connection to the county's data network. General access to the internet for personal use through the county network or Data Assets is strictly limited to Users. When accessing the county network from a personal computer, Users are responsible for preventing access to any county Data Assets by other individuals. Performance of illegal activities through the county network or Data Assets by any User is prohibited.

10. **Internet and Social Media Usage.** Internet usage including social media is owned and operated by the county. Internet usage is intended for normal county business operation purposes. Personal social media use is not allowed during work hours while working on the county's Data Assets. Postings to social networking platforms, including but not limited to, social media, chat rooms, blogs, and forums from a county device, from a personal device while using county Data Assets, or using a county email address are prohibited with the exception of those authorized or designated by the county to be posted on its behalf.

11. **Additional Measures.** The county is committed to keeping threats of security breaches to a minimum and enlists the support of all Users. Users are requested to:
   (a) Report any stolen or damaged equipment as soon as possible to the County Administrator, IT Manager, or designee;
   (b) Lock devices and turn off screens when leaving their workstations;
   (c) Contact the County Administrator, IT Manager, or designee immediately when a device is lost;
   (d) Avoid suspicious websites; and,
   (e) Not download suspicious, unauthorized, or illegal software on county devices.

12. **Privacy.** Users shall have no expectation of privacy for any information they store, send, receive, or access on the county's Data Assets. The county may monitor and inspect all Data Assets of any User without prior notice, in the course of an investigation triggered by indications of misconduct, or on random basis.

13. **Data Backup.** County data will be backed-up on a regular basis. Backups of data where loss would impact the operation or viability of the county will be taken off-site or written off-site to a secure location in a timely manner. Management of the offsite facility should follow the county's data classification policy and data retention, storage, and disposal practices. The county should ensure that offsite arrangements are periodically assessed, at least annually, for content and security. The county should confirm compatibility of hardware and software to restore archived data, and periodically test and refresh archived data.

14. **Data Retention and Disposal.** To provide a comprehensive range of services to the residents of the county, the retention, storage, and disposal of data will be undertaken at appropriate times, with adequate methods to meet legal, regulatory, and any other significant requirements. The county needs to process data and use documentation to be able to provide its services. This requires information to be stored in systems that enable it to honor contracts and other agreements. The county will only hold data and documentation for as long as required and will deploy an effective review mechanism to ensure that this works in practice based on data classification. The county will ensure compliance with all necessary legal and regulatory requirements regarding data and document retention, storage, and disposal. When establishing and/or reviewing retention periods, the following will be considered:
    (a) Local Government Records Commission retention, recommendations, and disposition;
    (b) The objectives and requirements of the county;
    (c) The class of data in question;
    (d) The purpose(s) for which the data in question is collected, held, and processed;
    (e) The county's legal basis for collecting, holding, and processing that data; and,
    (f) Anticipated or pending litigation.

15. **Disciplinary Action.** Disciplinary action may be taken against Users who expose the county to security breaches. Violation of this policy can lead to disciplinary action up to and including termination. The county's disciplinary protocols are based on the severity of the violation. Unintentional violations may only warrant a verbal warning. Frequent violations of the same nature, however, can lead to a written warning. Intentional violations can lead to suspension or termination of employment, depending on the case circumstances. Users may also be exposed to personal liability.

I-H(B). Social Media Policy and Procedure

Social media can be an effective communication tool for the county commission and its instrumentalities, departments, and agencies (collectively "County"). Improper usage of social media, however, may impact the County and affect the public trust in and credibility of the County. The County recognizes and respects the rights of its employees to participate in social media platforms. Employees, however, must ensure that their online content is consistent with the County's standards of conduct. In order to provide guidelines for acceptable and reasonable practices, policies, and procedures for social media communication, the Cullman County Commission hereby establishes this Social Media Policy and Procedure.

The purpose of this policy is to (a) define the parameters for both official and personal use of social media, (b) provide for the retention and disposal of social media postings and comments, and (c) list the County's disciplinary process for policy violations.

This policy applies to all county commission offices and county-funded instrumentalities, departments, and agencies, including but not limited to, the Revenue Commissioner's office, the probate office, and any other county-funded entity or program, and applies to permanent and part-time employees, remote workers, third-party agents, contractors, consultants, volunteers, suppliers, interns, and any individuals ("Users") who have permanent or temporary access to the County's social media platforms, sites, or pages**.** This policy applies to all social media communications whether or not an employee or User is posting under his or her name, anonymously, or through an alias or other means and to such communication and usage on personally-owned devices whether connected by wire or wireless service to the county network. This policy also applies to social media communication and usage on devices purchased using any officials' discretionary funds.

1. Definitions

(a) **Social Media**: All means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, forums, comment sections, and private or direct messages, whether or not associated or affiliated with the County, as well as any other form of electronic communication.

(b) **Official County Email Account**: Email account provided by a County instrumentality, department, or agency mail system or approved external mailbox that is used for official county business.

(c) **County Approved Social Media Account**: A social network that has been assessed and approved by the county administrator, the information technology (IT) department, the county attorney and human resources director, and/or the county department head or agency head.

(d) **Social Network**: Online platforms, sites, or pages, where profiles are created, information is shared, and parties socialize with each other using a range of electronic communication and technologies.

(e) **Page**: The portion of the social media network or platform where content is displayed, usually by a person with administrator rights.

(f) **Post**: A submitted or published message or blog in the form of, but not limited to, text, videos, photographs, graphics, links, including hyperlinks, documents, and computer applications.

(g) **Profile**: Information provided about a person or the County on a social networking platform, site, or page.

(h) **Comment**: A submitted or published response to a post.

2. **County Social Media Use and Management.** County-sponsored social media usage shall be limited to those with an official County business and purpose to use social media. County-sponsored and social media platforms, sites, or pages for County instrumentalities, departments, and agencies should be reviewed and approved by the county administrator, the information technology (IT) department, the county attorney, the human resources director, and/or the county department head or agency head. Any County-sponsored and approved social media platform, site, or page should be clearly identified with the following phrase: "Official social media site of 'department name," including a link to the County or department website and should include the County, department, or agency logo. A disclaimer should be placed on the platform, site, or page indicating that information included in posts and originating device identification information may be subject to public record disclosure and shall be recorded and archived. The County should designate a person who is responsible for

social media communications, including but not limited to, determining what information is posted on the platform(s), site(s), or page(s), and updating, commenting, reviewing, and auditing the content. The County should also identify backup personnel for times the designated person is unavailable. Designated personnel participating in social media discussions related to county business matters during off-County time shall indicate that viewpoints shared are personal and do not necessarily reflect County opinion. Any County-sponsored and approved social media platform(s), site(s), or page(s) should comply with all federal, state, and local laws.

3. **Personal Use of Social Media.** Employees or Users have the right to speak and act on social media on their own time as private citizens on matters of public concern. However, the following actions are forbidden, including but not limited to, regardless of whether an employee or User is on his or her own time:
    (a) Disseminating or discussing any information accessed because of an employee's or User's position that is not generally available to the public, including, but not limited to, confidential information regarding citizens or co-employees, or other Users; information regarding safety and security plans or procedures; information regarding expected or pending legal matters; or information regarding contract negotiations;
    (b) Releasing any media including, but not limited to pictures, videos, and audio recordings, obtained during the performance of an employee's or User's duties, agency-related activities, and agency-responder activities, unless prior approval is obtained;
    (c) Stating, suggesting, or implying in any manner that an employee or User is acting or speaking on behalf of the County without prior express authorization;
    (d) Violating the County's policies against harassment or discrimination;
    (e) Taking any other action that may reasonably be expected to interfere with the employee's or User's job duties or the County's operations;
    (f) Being disrespectful of the County, its employees, and its services or posting any material that is obscene, vulgar, defamatory threatening, discriminatory, harassing, abusive, hateful or embarrassing to another person or entity; and
    (g) Engaging in any activity that reflects or may reflect negatively on the County, its employees, or its services.

4. **Email and Internet Social Media Usage.** Employees are generally expected to work during all work times and should refrain from engaging in personal activities during work hours except for breaks. Personal use of electronic mail, social media, etc., that interferes with an employee's performance of his or her job duties is strictly prohibited. Any use of county resources, including, but not limited to, county equipment or bandwidth, for personal use may result in any information regarding the use, including metadata and data, to become public, and employees and Users have a decreased expectation of privacy in personal devices brought onto County property.

5. **Data Retention and Disposal.** The County will ensure compliance with all necessary legal and regulatory requirements regarding retention, storage, and disposal of any information posted and received through social media. When establishing and/or reviewing retention periods, the following will be considered:
    (a) Local Government Records Commission retention, recommendations, and disposition;
    (b) The objectives and requirements of the county;
    (c) The class of data in question;
    (d) The purpose(s) for which the data in question is collected, held, and processed;
    (e) The county's legal basis for collecting, holding, and processing that data; and
    (f) Anticipated or pending litigation.

6. **Disciplinary Action.** Disciplinary action may be taken against employees and Users who violate this policy. Violation of this policy can lead to disciplinary action up to and including termination. The county's disciplinary protocols are based on the severity of the violation. Unintentional violations may only warrant a verbal warning. Frequent violations of the same nature, however, may lead to a written warning. Intentional violations can lead to suspension or termination of employment, depending on the case circumstances. Employees and Users may also be exposed to personal liability.

I-H(C). Data Breach Notification Policy and Procedure

Pursuant to the Alabama Data Breach Notification Act of 2018, codified in Ala. Code § 8-38-1 et seq., all counties are required to have systems designed to secure all sensitive personally identifying information (SPII) as defined in Ala. Code § 8-38-2(6) or sensitive data ("sensitive data") during its lifecycle. This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

A data breach incident is a suspected or actual event that may adversely impact the confidentiality, integrity, or availability of county data, computer equipment, applications, systems, networks, media storage, and other technology infrastructure (collectively "Data Assets") or any information processed, stored, or transmitted by Data Assets. A data breach incident may include, but is not limited to:

(a) Loss or theft of sensitive papers or hard copies;
(b) Data emailed or faxed to the incorrect recipient;
(c) Loss or theft of equipment on which data is stored;
(d) Inappropriate sharing or dissemination of data;
(e) Hacking, malware, or data corruption;
(f) Information obtained by deception;
(g) Equipment failure, fire, or flood; and,
(h) Non-secure disposal of data.

Prompt detection, investigation, and appropriate handling of these incidents is necessary to protect Data Assets critical to the county, to preserve sensitive data privacy and confidentiality, and to facilitate compliance with the law.

In order to standardize the county's response to any data breach or information security incident and ensure that responses are appropriately logged and managed in accordance with the law and best practice, the Cullman County Commission hereby establishes this Data Breach Notification Policy and Procedure to be utilized in the event of a data breach or information security incident.

The purpose of this policy is to define the minimum requirements and responsibilities for detecting, investigating, assessing, and reporting data breach and information security incidents to minimize the negative impact on the confidentiality, integrity, and availability of the county's Data Assets.

This policy applies to all county commission offices and departments, including but not limited to, the Sheriff's office, the Revenue Commissioner's office, the probate office, and any other county-funded entity or program, and applies to permanent and part-time employees, remote workers, third-party agents, contractors, consultants, volunteers, suppliers, interns, and any other individuals who have permanent or temporary access to the county's Data Assets (collectively "Users"). This policy applies to all Data Assets and technology infrastructure, whether it is owned or leased by the county, and to personally-owned devices connected by wire or wireless service to the county network. This policy also applies to Data Assets purchased using any officials' discretionary funds. This policy relates to all sensitive data controlled or processed by the county regardless of format.

1. **Good Faith and Prompt Investigation.** When a data breach or security incident is detected or reported, key first steps are to investigate and determine (1) the scope of the breach; (2) whose information was compromised and the nature of that information; (3) whether the breached information is reasonably likely to cause substantial harm; and, (4) measures to be taken to restore security of the information and the system breached.

   In determining whether the breach is reasonably likely to cause substantial harm, consideration may be given to the following factors:

   (a) whether the information is in the physical possession and control of an unauthorized person;
   (b) whether the information has been downloaded or copied;
   (c) whether the information was used by an unauthorized person; and/or,
   (d) whether the information has been made public.

2. **Containment, Reporting, and Containment.** The county's first response to a cybersecurity threat shall be to isolate the infected Data Assets. This may range from removing the infected Data Assets from the network to severing all connections to other domains in response to a cyber incident. The individual committing the breach or having identified a possible breach should immediately inform the County Administrator, IT Manager, or designee. The immediate priority is to contain the breach and limit its scope and impact.

   Where sensitive data has been seen, accessed, or been sent to a person who does not have a legitimate need to see it, Users should contact the recipient and proceed as follows:
   (a) Instruct the recipient not to disseminate the data or discuss it with anyone else;
   (b) Tell the recipient to destroy or delete the data they have received and confirm the action in writing; and,
   (c) Warn the recipient of any implications if they further disclose the data.

   Where data has been lost, altered, or has become unavailable, access to the data should be resumed as quickly as possible via backup copies of the data, if available.

   A data breach detection, investigation, or incident should be logged stating:
   (a) Date and time of the breach;
   (b) Date and time the breach was detected;
   (c) Who committed the breach;
   (d) Details of the breach;
   (e) Approximate number of individuals involved in the breach;
   (f) Whether the breach was reasonably likely to cause substantial harm; and,
   (g) Details of actions already taken in relation to containment and recovery.

   All records relating to the determination of whether the breach was "reasonably likely to cause substantial harm" must be maintained by the county for five (5) years.

3. **Assessing the Risks.** The County Administrator, IT Manager, or designee will conduct an investigation to assess the risks and will prepare a report. This report will consider the following:
   (a) How the breach occurred;
   (b) The type of data involved;
   (c) The number of and the individuals affected by the breach;
   (d) The sensitivity of the data breached;
   (e) The potential harm to the individuals affected;
   (f) The possible effect if the sensitive data is used inappropriately or illegally;
   (g) For sensitive data that has been lost or stolen, whether there were any protections in place such as encryption;
   (h) The measures taken or proposed to be taken to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects; and,
   (i) Whether notification of the breach should be provided.

   Once the breach has been assessed, security measures may be a need to be updated and additional training may need to be conducted.

4. **Notification to Affected Individuals.** When the investigation indicates that sensitive data has been, or is believed to have been, acquired by an unauthorized person and is likely to cause substantial harm to the individuals who are the subject of the information, notification must be provided to the affected individuals, without undue delay, particularly if there is a need to mitigate any immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach. All individuals affected by a data breach must be directly notified in writing as quickly as possible, but no later than forty-five (45) days after making the determination that notice is required or receiving notice from

a third-party agent that a breach has occurred. Notification must be sent to the mailing address or email address the county has on file for the individual, and should include at least the following information:

(a) The date, or estimated date of the breach;
(b) A description of the sensitive data that was acquired from the breach;
(c) A general description of the actions taken by the county to restore the security and confidentiality of the personal information subject to the breach;
(d) A general description of the steps affected individuals can take to protect themselves from identity theft; and,
(e) Contact information for the county's designee related to the breach.

Substitute notice in lieu of direct notice may be given if at least one of the following circumstances is met: (1) the cost of providing direct notice would exceed $500,000 or is an excessive amount relative to the resources of the covered entity, (2) there is insufficient contact information for the individuals requiring notification, or (3) over 100,000 people were affected by the data breach. Substitute notice, when allowable, can be satisfied by placing it in a conspicuous location on the county's website, if available, for 30 days or through print and broadcast media outlets. Substitute notice methods may also be approved by the Attorney General.

Notification may be delayed when requested by federal or state law enforcement based on a criminal investigation or national security issues. If the county's investigation determines that notification to affected individuals is not required, all records relating to that determination must be maintained by the county for five (5) years.

5. **Notification to the Attorney General.** If a data breach impacts more than 1,000 people, the county must notify the Attorney General no later than forty-five (45) days after making the determination that notice is required or after receiving notice from a third-party agent that a breach has occurred. The county must provide the Attorney General with:

(a) A summary of the events surrounding the breach;
(b) The estimated number of Alabama residents impacted by the breach;
(c) A list of any free services being offered to individuals affected by the breach along with instructions on how to use the services; and
(d) The contact information of the county designee from whom additional information may be obtained about the breach.

Any information provided to the Attorney General that is marked as confidential will not be subject to any requests under the open records law.

6. **Notification to Credit Reporting Agencies.** If a security breach impacts more than 1,000 people, the county must notify, without reasonable delay, "all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis…of the timing, distribution, and content of the notices."

7. **Disciplinary Action.** Disciplinary action may be taken against Users who expose the county to security breaches. Violation of this policy can lead to disciplinary action up to and including termination. The county's disciplinary protocols are based on the severity of the violation. Unintentional violations may only warrant a verbal warning. Frequent violations of the same nature, however, can lead to a written warning. Intentional violations can lead to suspension or termination of employment, depending on the case circumstances. Users may also be exposed to personal liability.

Cullman County Data or Cybersecurity Incident Reporting Form

Instructions: In the event of a Data or Cybersecurity Incident, this form should be completed as soon as possible and given to the County Administrator, IT Manager, or other person designated by the County Commission to protect against data security breaches. The report should then be brought to the attention of the County Commission.

1. Contact Information for Person Reporting Incident.

Name	
Title	
Office/Department	
Phone Number	
Email Address	

2. Incident Description. Provide a brief description of the incident, including how the incident was detected and what occurred.

_____

_____

3. Incident Details.

Date and Time Incident was Discovered	
Type of Information Involved: Sensitive, Restricted, or Public (see definitions below)	
Has the Incident Been Resolved?	
Source/Cause of the Incident, If Known	
Mitigating Factors	
Approximate Number of Individuals Affected	

Type of Information Involved: Sensitivity Classifications.

Category of Information	Definition
Sensitive information	Alabama resident's first name or first initial and last name, in combination with any one of the following: • A Social Security number or tax identification number; • A driver's license number or any other unique, government-issued identification number used to verify identity; • Any financial account number in combination with access information (e.g., a security code, expiration date, or PIN); • Any information regarding a person's medical, mental or physical history, condition or treatment; • A person's health insurance policy number or subscriber identification number and unique identifier; or,

	• A username or email address, in combination with a password or security question and answer.
Restricted Information	Internal use information that must be guarded due to custody, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal mandates, unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of information could cause monetary loss, damage to the county's reputation, or violate an individual's privacy rights (e.g., educational records, employment history, and biographical information).
Public Information	Information that is not publicly disseminated, but accessible to the public. This data is either explicitly defined as public information (e.g., employee salary ranges), intended to be readily available to individuals both on and off premises (e.g., an employee's work email address), or not specifically classified elsewhere as protected information. Publicly available information may be subject to appropriate review or disclosure procedures to mitigate potential risks of inappropriate disclosure of data or to organize it according to its risk of loss or harm from disclosure.

4. **Impact or Potential Impact.** Check all that apply.
   - ☐ Loss or Compromise of Information
   - ☐ Damage to Systems
   - ☐ System Downtime
   - ☐ Financial Loss
   - ☐ Other Organization's Systems Affected
   - ☐ Interference with County Operations
   - ☐ Unknown

5. **Incident Notification.** Has anyone been notified of this incident? If yes, provide their name and title.

_____

6. **Do you have a reasonable belief that sensitive information has been acquired by an unauthorized person and is reasonably likely to cause substantial harm to individuals to whom the information relates?** Examples: (1) information is in the physical possession and control of an unauthorized person; (2) evidence that information was downloaded or copied; (3) evidence that information was used by an unauthorized person; (4) whether the information has been made public.

_____

_____

7. **Response.** What actions have been taken in response to this incident so far?

_____

_____

What can be done to avoid incidents like this in the future?

_____

_____

Cullman County Commission Cybersecurity Acknowledgement Form

The Cullman County Cybersecurity Manual describes important information about Cullman County's data, cybersecurity, social media, and data breach notification. I understand that I should consult my immediate supervisor or the county IT Director or HR Manager regarding any questions not answered by the Cybersecurity Manual.

Since the information described in the Cybersecurity Manual is necessarily subject to change, I acknowledge that revisions to the policies and procedures may occur. All such changes will be communicated through official notices, and I understand that the revised information may supersede, modify, or eliminate existing policies and procedures.

Furthermore, I acknowledge that these Cybersecurity Policies and Procedures are neither a contract of employment nor a legal document. I have reviewed the Cybersecurity Policies and Procedures, and understand that I may ask any questions I might have. I accept the terms of the Cullman County Cybersecurity Policies and Procedures. I also understand that it is my responsibility to read and comply with the policies contained therein and any revisions made to it in the future. I further agree that if I remain employed with Cullman County following any modifications to the Cybersecurity Policies and Procedures, I thereby accept and agree to such changes.

I hereby acknowledge that the Cullman County Cybersecurity Policies and Procedures provided to me on this day are in addition to those listed in the Cullman County Personnel Policies and Procedures (employee handbook). I understand that should a conflict exist between the Cullman County Cybersecurity Policies and Procedures and procedures from the Cullman County Personnel Policies and Procedures (employee handbook), the Cullman County Cybersecurity Policies and Procedures shall supersede.

I understand that this form will be retained in my personnel file.

_____ _____

Employee Signature Employee Name

_____

Date

PLEASE SIGN ACKNOWLEDGEMENT FORM ON BACK PAGE OF THIS BOOKLET.

Cullman County Commission
500 2nd Ave SW
Cullman, AL 35055

Cullman County Commission Cybersecurity Acknowledgement Form

The Cullman County Cybersecurity Manual describes important information about Cullman County's data, cybersecurity, social media, and data breach notification. I understand that I should consult my immediate supervisor or the county IT Director or HR Manager regarding any questions not answered by the Cybersecurity Manual.

Since the information described in the Cybersecurity Manual is necessarily subject to change, I acknowledge that revisions to the policies and procedures may occur. All such changes will be communicated through official notices, and I understand that the revised information may supersede, modify, or eliminate existing policies and procedures.

Furthermore, I acknowledge that these Cybersecurity Policies and Procedures are neither a contract of employment nor a legal document. I have reviewed the Cybersecurity Policies and Procedures, and understand that I may ask any questions I might have. I accept the terms of the Cullman County Cybersecurity Policies and Procedures. I also understand that it is my responsibility to read and comply with the policies contained therein and any revisions made to it in the future. I further agree that if I remain employed with Cullman County following any modifications to the Cybersecurity Policies and Procedures, I thereby accept and agree to such changes.

I hereby acknowledge that the Cullman County Cybersecurity Policies and Procedures provided to me on this day are in addition to those listed in the Cullman County Personnel Policies and Procedures (employee handbook). I understand that should a conflict exist between the Cullman County Cybersecurity Policies and Procedures and procedures from the Cullman County Personnel Policies and Procedures (employee handbook), the Cullman County Cybersecurity Policies and Procedures shall supersede.

I understand that this form will be retained in my personnel file.

_____ _____

Employee Signature Employee Name

_____

Date

Cullman County Commission
500 2nd Ave SW
Cullman, AL 35055