Official Records of Morgan County, CO 915418
11/20/2018 11:08:57 AM Pgs: 7 Rec Fee: 0.00
State Documentary Fee: $ Clerk: Susan L. Bailey

MORGAN COUNTY, COLORARDO
BOARD OF COUNTY COMMISSIONERS

RESOLUTION 2018 BCC 43

A RESOLUTION OF THE BOARD OF COUNTY COMMISSIONERS OF MORGAN COUNTY ADOPTING A DATA PROTECTION POLICY AS REQUIRED BY HOUSE BILL 18-1128.

WHEREAS, the State of Colorado has enacted House Bill 18-1128 (the "Act"), effective September 1, 2018, which requires all Colorado governmental entities to I) create a written data disposal policy reasonably calculated to protect personal identifying information[1] of Colorado residents maintained in County records from unauthorized disclosure, II) maintain adequate security protections for the same purpose, III) follow specific procedures to notify affected Colorado residents if their personal information[2] may have been compromised by an unauthorized breach of the County's records, and IV) ensure that third-party service providers comply with the requirements and standards of the Act; and

WHEREAS, in the ordinary course of government business, various Morgan County Departments maintain hard copy files, computer devices, and electronic media that contains personal identifying information and personal information as defined in House Bill 18-1128.

NOW, THEREFORE, in consideration of the premises and requirements under the Act, it is resolved that Morgan County adopts the following policies:

I. Computer Security Incident Notification Policy

A. Computer Security Incident (CSI) Defined

For the purpose of this policy, a Computer Security Incident ("CSI") is defined as a violation or imminent threat of violation of computer security policies that may result in an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information.

B. Colorado Resident Defined

For the purpose of this policy, a Colorado resident is defined as an individual who resides in Colorado for 90 consecutive days immediately preceding the CSI or who was domiciled in the state on the date of the CSI. A person's domicile is in Colorado if the person's place of abode is in Colorado and that person, whenever absent, has the present intention of returning after a departure or absence, regardless of the duration of the absence.

---

[1]House Bill 18-1128 (C.R.S. § 6-1-713.5) defines "personal identifying information" as a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, as defined in section 6-1-716 (l)(a); an employer, student, or military identification number; or a financial transaction device, as defined in section 18-5-701 (3).

[2] House Bill 18-1128 (C.R.S § 6-1-716) defines "personal information" as I) a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: social security number; driver's license number or identification card number; student, military, or passport identification number; medical information; health insurance identification number; or biometric data, as defined in section 24-73-101(1)(a), II) a Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account, or III) a Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

Any County employee or contractor who discovers that a CSI may have occurred must immediately report the incident to the responsible elected official or department head. The elected official or department head must immediately contact their internal information technology ("IT") administrator and their third-party IT contractor.

D. Information Technology Contractors Must Follow NIST Standards

All third-party contractors who contract with Morgan County in providing IT services related to a CSI must apply the industry standards issued by the National Institute of Standards and Technology ("NIST"), Computer Security Incident Handling Guide, Special Publication 800-61 or a similar industry standard.

E. County Attorney Must Be Notified

Immediately upon discovering, through IT investigation, that a CSI may have occurred, the responsible elected official or department head must immediately notify the County Attorney.

F. Public Information Officer Must Notify Affected Parties Within 30 Days

Once the affected Colorado residents of a CSI are ascertained, the County Public Information Officer shall notify the Colorado residents according to the manner of notice requirements of C.R.S. § 24-73-103, *et seq.*, not later than (30) thirty days after confirming that a CSI may have occurred. Notification may be delayed only if a law enforcement agency determines that notice will impede an ongoing criminal investigation, but must be provided within thirty (30) days after the law enforcement agency determines that notification will no longer impede the investigation.

G. Public Information Officer Must Notify Other Parties Within 30 Days

In accordance with C.R.S. § 24-73-103, *et seq.*, and in addition to the affected parties, notice of a CSI shall be provided to the Colorado Attorney General if it is reasonably believed that a CSI affected five hundred (500) or more Colorado residents. Such notice shall be provided within thirty (30) days after the date of determination that a CSI has occurred. Additionally, notice of a CSI shall be provided to all consumer reporting agencies that compile and maintain files of consumers on a nationwide basis if it is reasonably believed that a CSI affected one thousand (1,000) or more Colorado residents.

H. Application to Third-Party Service Providers

Third-party service providers who store, maintain, or process personal information for or on behalf of Morgan County must give notice to and cooperate with the County in the event of any CSI. Notice to the County shall be provided in the most expedient time possible and without unreasonable delay, and any information relevant to the CSI shall be disclosed. A Third-party service provider's refusal to comply with this Section H shall be a violation of C.R.S. § 24-73-103(2)(g) and could be subject to legal action by the Colorado Attorney General.

II. Data Disposal Policy

A. Purpose

The purpose of this data destruction policy is to prevent the unauthorized disclosure of personal identifying information by properly destroying print media and properly removing the information stored on electronic media. The reuse, recycling or disposal of computers and other devises storing data poses a significant risk because data can easily be recovered even if the data files were deleted or a hard drive has been reformatted. When personal identifying information is no longer needed, or the device storing such information becomes obsolete, the information should be irreversibly destroyed in accordance with this policy. Failure to properly purge data may result in unauthorized access in violation of state and federal laws.

B. Scope

This policy applies to the Morgan County government community, including all employees, elected officials, interns, contractors and vendors.

C. Print and Electronic Media Defined

This policy applies to both print and electronic media. Electronic media means intangible computerized data and includes the tangible equipment on which the intangible data is stored or was once stored, including but not limited to computer hard drives, smartphones, desktops and laptops, USB storage drives, CDs and DVDs, and zip drives. Print media means physical documents, including notes or records that are computer printed, copied, handwritten or otherwise manifested into tangible form.

D. Disposal Procedures

When print or electronic media, documents, or equipment that contain or once contained Personal Identifying Information are no longer needed, as determined by a records retention schedule, the County shall destroy or arrange for the destruction of such documents or equipment that remain under its custody or control in a manner consistent with this policy.

Print media that contains or once contained personal identifying information shall be disposed of by one (or a combination) of the following methods:

i. *Shredding.* Shredding using cross-cut shredders;
ii. *Shredding Bins.* Disposal using locked bins located on-site using a licensed and bonded information disposal contractor; or
iii. *Incineration.* Physically destroyed using a licensed and bonded information disposal contractor contracted.

Electronic media that contains or once contained personal identifying information shall be disposed of by one of the following methods:

i. *Overwriting Magnetic Media.* Overwriting uses a program to write binary data sector by sector onto the electronic media that requires sanitization, with a minimum of three passes;
ii. *Degaussing.* Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state; or
iii. *Physical Destruction.* Implies complete destruction of Electronic Media by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated.

Destruction of hard drives shall be conducted on-site by two or more IT or Administrative County staff members who will destroy, witness and record destruction of electronic storage media. Inoperable electronic storage media shall be disposed of by physical destruction.

Any technology that handles protected health information covered by HIPAA shall not be released from Morgan County's control until the equipment has been sanitized and all stored information has been cleared using methods in accord with the HIPAA Security Final Rules, Section 164.310, Physical Safeguards, Part (d), (1) &(2).

E. Reduce Volume of Personally Identifiable Information

Each elected official or department head must review their current holdings of personal identifying information and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely and complete, and reduce them to the minimum necessary for the proper performance of the department functions.

Following initial review, Morgan County Departments must periodically review their holdings of sensitive material that contain personal identifying information. For departments using retention policies established by the State of Colorado, adherence to the retention policy satisfies this requirement.

F. State of Colorado Records and Retention Policies

This policy is intended to supplement, and not conflict with, applicable retention policies established by the State of Colorado. All elected officials and department heads shall continue to implement the records retention policies established by the State of Colorado for their respective offices. If for any reason a conflict arises between the State of Colorado retention policy and this Morgan County policy, the retention policy shall control.

G. Application to Third-Party Service Providers

Any contract with a third-party service provider for the disposal or recycling of Electronic Media or Print Media must contain a provision verifying that the Third-Party Service Provider has procedures for proper disposal in accordance with C.R.S. § 24-73-101(1), as amended.

III. Data Protection and Security Procedures Policy

A. Purpose

The County is responsible for activities that require the collection of confidential or sensitive Colorado resident data. The County has adopted the policy below to reasonably protect Colorado Resident Personal Identifying Information that is collected, used, shared, and stored by the County.

B. Use of Computers and Passwords

Only County employees and other specifically approved persons are authorized to use or access the County's computers. Employees may only use computer software and related equipment in the direct performance of their assigned duties. The County has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media to ensure compliance with this Policy and state and federal law. All employees shall have an individual password that allows them to access the system. An employee may not share or offer the use of his or her password, and unauthorized use of another employee's password is prohibited. Should an employee believe their password has been compromised or made available to others, they must immediately reset/change their password and notify the information systems director.

C. Use of Electronic Mail

All electronic mail ("email") sent by an employee on behalf of the County or in the performance of employment tasks shall be sent from the employee's password protected official email account, and no personal accounts shall be used to complete employee duties. Each email sent from a County account shall include a signature stating that the message is confidential and intended only for the individual for which it was addressed, that error should be reported to the sender, and that disclosure or use of the email contents or attachments is prohibited. Email passwords shall not be shared and unauthorized use of another employee's email account is prohibited. Each employee provided with an email account acknowledges that the County reserves the right to monitor email messages (including personal/private/instant messaging systems) and their content, as well as any and all use of the Internet and of computer equipment used to create, view, or access email and Internet content. Employees must be aware that the email messages sent and received using County equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by the County at any time.

D. Internet Connection and Online Activity

The Internet represents a potentially destructive source for computer viruses and poses a particular threat to maintaining the integrity and safety of County-held data that contains Personal Identifying Information;

therefore, great care must be taken regarding any files that are downloaded. All users with Internet access must have current anti-virus software running at all times, as set forth in Section 5(E) hereof. Downloaded files (word processing documents, spreadsheets/charts, images, etc.) must be scanned with current antiviral software before execution or first use. Use of County computers, networks, and Internet access is a privilege and access may be revoked for inappropriate conduct, including without limitation:

i. Failing to log off any secure, controlled-access computer or other form of electronic data system to which the employee is assigned, if the employee leaves such computer or system unattended;
ii. Causing congestion, disruption, disablement, alteration, or impairment of the County's networks or systems;
iii. Engaging in unlawful or malicious activities that violates the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
iv. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the County's networks or systems or those of any other individual or entity; and
v. Defeating or attempting to defeat security restrictions on County systems and applications.

E. Antivirus and Malware

All workstation and server based assets used for County business, whether connected to the County network or as standalone units, must use County approved antivirus/antimalware protection software and configuration provided by the County. To ensure the integrity and safety of Personal Identifying Information held by the County and minimize the risk presented by viruses and malware, the following prohibitions are in place:

i. Settings for the virus protection software must not be altered in a manner that will reduce the software effectiveness;
ii. Virus protection software must not be disabled or bypassed; and
iii. Automatic update frequency cannot be altered to reduce the frequency of updates.

Any threat that is not automatically cleaned, quarantined, and subsequently deleted by malware protection software must be reported to the information systems director. If an employee suspects that the system may be infected, the following actions must be taken:

i. Inform County information systems department and departmental management immediately;
ii. Switch off the machine;
iii. Take appropriate measures to ensure no-one uses the machine; and
iv. Inform County information systems department and departmental management of any actions taken which may have caused the infection.

F. Network Device Security and Use of Network Server

Network services are an essential component of the County's information resources. Routers and switches physically (and virtually) separate logical networks through configuration and protocol management. Effective management of these important network devices helps to protect internal network resources from external risks, so:

i. Areas where physical network components reside shall be secured at all times to prevent unauthorized access or tampering;
ii. All Personal Identifying Information must be stored on the County's network, and may not be stored on desktops or in temporary folders;
iii. The County will perform regular backups of user files stored on the County's network servers; and
iv. Employees may be permitted access only to approved County resources and systems and may be restricted from accessing certain documents and folders on the network that contain sensitive information.

County employees or users who are not involved directly in information security systems management shall not:

i. Extend or re-transmit County network services by installing a router, switch, hub, or wireless access point on any County-administered network;
ii. Install any network hardware or software that provides network services without the express authorization of the information systems director;
iii. Alter network hardware in any way; or
iv. Download, install, or run security programs or utilities that reveal weaknesses in the security of a system unless authorized by the information systems department.

G. Remote Access and Personal Devices

Employees shall not bring personal computers to the workplace or connect them to County electronic systems or the network unless expressly permitted to do so. If permission to bring personal devices to work to perform employee duties is granted, or if permission to connect a device for remote access to the network is granted, the employee's personal device becomes subject to the requirements of this Policy and the employee is responsible for ensuring compliance. Access may be restricted on certain applications and data sources that, due to their sensitive nature, may not be accessed by personal devices. The use of portable flash drives is prohibited without the express written permission of the County information systems department.

H. Workstation Security

Employees shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access at their workstations. Physical access to workstations shall be restricted to authorized personnel. Employees shall prevent unauthorized viewing of information on a screen by:

i. Ensuring monitors are positioned away from public view;
ii. If necessary, installing privacy screen filters or other physical barriers to prevent public viewing;
iii. Manually activating a password protected screen saver when leaving the workstation;
iv. Exiting running applications and closing any open documents; and
v. Ensuring workstations are logged off at the end of each business day.

I. Employee Termination

When an employee retires, is terminated, or otherwise leaves employment with the County, access to systems and applications will be immediately terminated. Employee work records and data stored locally or on servers shall be preserved. Accounts of individuals on extended leave (more than 30 days) shall be temporarily disabled. Termination of employment shall be classified as either friendly or unfriendly. Friendly terminations occur when an employee departs employment with the County on agreeable terms with no reasonable expectation of posing a risk that would result in a Security Breach, and procedures are as follows:

i. Remove access privileges and computer accounts within a reasonable time of termination;
ii. Repossess access keys to the office and office furniture and equipment;
iii. Brief the departing employee on the continuing responsibilities for confidentiality and privacy;
iv. Instruct the employee to return all County property, work product, documents, and equipment; and
v. Insure interim or replacement staff's ability to access data.

Unfriendly terminations are events that have the potential for adverse consequences that may result in a Security Breach, so coordination between the termination of access and the termination of employment should occur, and procedures are as follows:

i. Remove access privileges and computer accounts as soon as possible, or if the employee is immediately terminated, remove system access at the same time or immediately prior to the notification and dismissal;
ii. Repossess access keys to the office and office furniture and equipment;

iii. Brief the departing employee on the continuing responsibilities for confidentiality and privacy;
iv. Instruct the employee to return all County property, work product, documents, and equipment; and
v. Communicate with the County Attorney to determine whether assets need to be preserved for legal review, chain of custody, or other investigative events.

J. Print Media Security

Print media containing Personal Identifying Information shall be stored in a secure location when not in immediate use, such as a locked cabinet or an unlocked cabinet in a locked room. Physical access to such documents should be sufficiently restricted to protect the information from those who do not have permission to access that material. Visitors should always be escorted and easily identifiable when in areas that may contain sensitive information. When Print Media containing Personal Identifying Information is no longer needed, it shall be disposed of in accordance with the Data Disposal Policy.

K. Application to Third-Party Service Providers

In accordance with C.R.S. § 24-73-102(2), any third-party service provider that stores, maintains, or processes personal identifying information on behalf of Morgan County must provide Morgan County written confirmation that the third-party service provider has implemented and maintains their own security and data breach prevention policy that is reasonably designed to protect personal identifying information from unauthorized access, use, modification, disclosure, or destruction and that the provider apply an industry standard substantially similar to the NIST, Computer Security Incident Handling Guide, Special Publication 800-61. If the Third-Party Service Provider does not have such a policy, or if such policy does not protect the disclosed information to the same extent or greater than does the County's policy, then the Third-Party Service Provider is required to follow the County's Data Protection and Security Procedures Policy to help protect Personal Identifying Information from unauthorized access, modification, disclosure, or destruction. Any contract with a Third-Party Service Provider shall contain such a requirement.

ADOPTED this 20th day of November, 2018

BOARD OF COUNTY COMMISSIONERS
MORGAN COUNTY, COLORADO

Mark A. Arndt, Chair

Laura D. Teague, Commissioner

James P. Zwetzig, Commissioner

MORGAN COUNTY SEAL COLORADO

ATTEST:

Susan L. Bailey
Morgan County Clerk to the Board