SUMMIT COUNTY
COLORADO

DATA PRIVACY PROTECTION POLICY

I. AUTHORITY:

A. C.R.S. § 24-73-101. Governmental entity - disposal of personal identifying information
B. C.R.S. § 24-73-102. Governmental entity - Protection of personal identifying information
C. CRS § 24-73-103. Governmental entity - notification of security breach
D. C.R.S. § 24-71.3-112. Retention of electronic records - originals

II. PURPOSE:

Various services at Summit County Government (the "County") need to gather information as a matter of business. C.R.S. § 24-73-101 *et seq.* requires governmental entities to create a policy for effectively managing the integrity of personal information with reasonable measures in place in the event of a data breach. This Data Privacy Protection Policy ("Policy") specifically addresses how to deal with "Personal Identifying Information (PII)" and "Personal Information (PI)" as defined below.

This Policy provides consistent guidelines for how the County deals with PII and PI in regard to appropriate gathering of paper and electronic data, how long that data remains in the possession of the County if not controlled by other law or expectation, and how that data is disposed when no longer needed or retained as required by superseding regulation. This Policy also outlines what notifications need to take place in the event of a data breach of PI pursuant to C.R.S. § 24-73-103. This Policy extends to any vendors or contractors that deal with this type of information as part of business agreements for a service.

III. DEFINITIONS:

A. Personal Identifying Information (PII) is a superset of personal confidential data defined as any of the following data elements:
    1. Social Security Number;
    2. Personal Identification Number;
    3. Password;
    4. Pass Code;
    5. Official state or government-issued driver's license or identification card number
    6. Government passport number;
    7. Biometric data (unique data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when accessing an online account);
    8. Employer, student, or military identification number; and
    9. Financial transaction device (any instrument or device such as a credit card, banking card, debit card, electronic fund transfer card, guaranteed check card, or account number representing a financial account).

B. Personal Information (PI) is a subset of PII defined as:
    1. A Colorado resident's first name or initial and last name in combination with any one or more of the following data elements if not encrypted, redacted, or secured by a means to render the name of the element unreadable or unusable that would, for example, permit access to an online account:
        a. Social Security number;
        b. Student, military, or passport identification number;
        c. Driver's license number or identification card number;
        d. Medical information (any information regarding medical or mental health treatment or diagnosis by a healthcare professional);
        e. Health insurance identification number; or
        f. Biometric data.
    2. A Colorado resident's username or email-address, in combination with a password or security questions and answers that would permit access to an online account; or
    3. A Colorado resident's account or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.
    4. PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government record or distributed media.

C. Retention: Refers to the time when data that is in a readable or usable format is in possession of County services or vendors/contractors. For example, a "retention schedule" outlines, for a specific set of data, when data records are to be disposed of.

D. Disposal: Refers to the arrangement or destruction of data by shredding, erasing, or otherwise modifying the PII unreadable or indecipherable through any means.

E. Notification: The procedure of realizing when a security breach occurs, identifying the type of data affected and the set of Colorado residents it affects, and making required notifications to affected Colorado residents as well as notification to the Colorado Attorney General.

F. Security Breach or Data Breach: The unauthorized acquisition of unencrypted computerized data or physical records that compromise the security, confidentiality or integrity of PI. This applies to the physical removal of paper records as well as, for example, a hard drive with data not effectively destroyed.

G. Data Subject: The person whose PII is being collected.

H. User: Any County employee or employee of a vendor/contractor who interacts with PII collected for County business in any manner during the course of their employment.

IV. SCOPE: This Policy and Procedure applies to all offices, service areas, departments, and divisions of the County and vendors/contractors who deal with PII associated with the County business processes.

V. RESPONSIBILITY: Data security is the responsibility of the individual dealing with PII, the office, service area, department, or division in which they operate, and the supporting security framework at the County administered by Information Systems. Offices, service areas, departments, and divisions should carefully determine if this information is critical to collect, and if it must be collected, have effective measures to control and keep this information confidential, and effectively dispose of it when no longer needed or required. Offices, service areas, departments, and divisions are also responsible for ensuring vendors/contractors who maintain PII comply with this Policy.

A. A department head, division head, or elected official shall be responsible for the general administration and implementation of a record retention schedule as determined appropriate by the department or office in conjunction with the Colorado State Archives requirements. Additionally, this role shall provide advisory services as required to facilitate communication amongst designated record custodians and technicians in the department or office to encourage and keep the County accountable to the tenets of this Policy. A department head, division head, or elected official shall act as the responsible authority within an office, service area, department, or division for ensuring departmental compliance relating to the retention and disposal of PII.
B. An office, service area, department, and division shall ensure compliance with this Policy.
C. An office, service area, department, and division shall make every effort to identify PII and how it relates to the intent of this Policy with respect to retention and disposal. They are also responsible for carrying out the external notification process in the event of a data security breach that affects PI.
D. The Information Systems (IS) Department, as part of its cybersecurity responsibility, will implement and maintain reasonable security procedures and practices to ensure that electronic data that has been identified as PII are adequately protected.
E. Offices, service areas, departments, and divisions are accountable to ensure vendor/ contractors compliance to this Policy.
F. Users who collect PII during the course of business shall be responsible for compliance with this Policy and respective retention schedules, notifying office, service area, department, or division leaders of any suspected data breach, and carrying out any data disposal as appropriate to their job function.
G. Users will insure sharing PII will only be done using appropriate tools and procedures as defined by federal regulations, Colorado State Statute, and County regulations, such as using approved encrypted email and secure file sharing services. PII is not to be shared informally outside of these tools and procedures.

VI. POLICY AND PROCEDURE: This section outlines the baseline requirements that responsible entities must follow in order to protect PII.

A. Data Security
   1. Users must do due diligence in respecting and maintaining appropriate controls to ensure PII is processed appropriately.
   2. Users will keep all data secure by taking reasonable precautions, following guidelines outlined within this Policy and any associated procedures in superseding laws or regulations.
   3. Data access permissions are determined based on the functional role of the County employee and existing access controls.
   4. The County will provide appropriate security awareness training to all employees that handle PII.
   5. PII will not be disclosed to any unauthorized person, either within the organization or externally.
   6. IS Department will utilize necessary physical and technical controls and organizational measures to ensure all infrastructure containing data is protected and secured.
   7. Users will follow associated procedures and notify relevant staff when reporting incidents or data breaches.
   8. Users shall collaborate with Information Systems in cases involving electronic data breaches.

B. Data Collection: Summit County and vendors/contractors should not collect PII unless required as a function of mandate or service delivery. The County and associated users or partners will collect PII only within established procedures and in accordance with the law.

C. Data Storage:
   1. The method in which PII in either electronic or paper format is stored must be secured from unauthorized use.
   2. When data is stored electronically, it must be reasonably protected from unauthorized access, accidental deletion, and malicious hacking attempts.
   3. Users should avoid storing PII on removable media. If data must be stored on removable media devices, it must be physically secured and encrypted.
   4. County data must be stored on designated drives and servers and users may only upload data to approved cloud computing services. Under no circumstances should PII be stored on local computer hard drives or storage devices.
   5. Servers containing PII must be situated in a secure location.
   6. Users should refrain from storing PII on paper. Users should only print when necessary, and destroy paper records when no longer needed.
   7. Paper records containing PII should be kept in a physically secure location when not being actively used.
   8. Users must ensure paper documents containing PII are not left in view of the public, for example, on a printer or on a desk. In addition, employees must ensure that

electronic PII is not visible to unauthorized people, such as on a monitor that the public may have the ability to view.

D. Data Use: The County and its vendors/contractors must work with Colorado residents to maintain transparency with Data Subjects regarding the use, processing, maintenance, and destruction of their PII by adhering to the following procedures:
   1. When working with PII, Users must ensure screens are locked when left unattended. The County IS Department must set screens to lock if inactive for more than 10 minutes by default.
   2. Users must not share PII that is held by the County unless the use is within the course of County business or operations.
   3. When possible, Users should retain only one copy of a record that contains PII, and access the record via original or master document.

E. Data Retention:
   1. PII should only be kept as long as needed or required by superseding regulations. Each office, service area, department, and division is responsible for identifying all physical or electronic records that contain PII and create a process for managing this information for appropriate use, visibility, and disposal.
   2. Data should be regularly reviewed against the applicable Colorado State Archives' records retention schedule. If no longer needed or required by state or federal law or regulation, data should be promptly and appropriately disposed.
   3. The IS Department must execute data backups alignment with an established backup and recovery schedule.
   4. Paper documents will be shredded and securely disposed or scheduled for destruction by a specialized vendor when no longer needed or required to be kept. Or, in the case where historical records must be kept without the associated PII, all PII must be effectively redacted.
   5. Any removable media, such as a hard drive, must be deleted and wiped using an approved wiping method, such as the NIST SP 800-88 media erasure guidelines.
   6. Data retention schedules or access with respect to PII are subject to superseding requirements from federal or Colorado State law as indicated, as contained, for example in HIPAA, CORA requests, and legal holds.

F. Notification Procedure for Data Breach
   1. If an office, service area, department, or division becomes aware of a potential data breach of records that contain PI, it is required to take appropriate action as defined in this section to investigate the cause and extent of the breach. The office, service area, department, or division will work in conjunction with other departments including IS, the Sheriff's Office, and County Attorney to launch and manage such an investigation.
   2. If the investigation determines that there is sufficient evidence to conclude that a security breach involves the misuse or reasonable likelihood of misuse of PI, the affected office, service area, department, or division must issue notice to affected Colorado residents. Notice must also be given to the Colorado Attorney General if

the security breach is reasonably believed to have affected 500 Colorado residents or more. Notice (enclosure A) must be given no later than 30 days after the date of determination that a security breach involving PI occurred. Notices to the Attorney General are sent to:

Office of the Attorney General
Consumer Protection Section
Colorado Department of Law
Ralph L. Carr Judicial Building
1300 Broadway, 7th Floor
Denver, Co 80203

3. The Notice must include the following information:
    a. The date, estimated date, or estimated date range of the security breach;
    b. A description of the PI that was acquired or reasonably believed to have been acquired as a result of the security breach;
    c. Information on how to contact the County to inquire about the security breach;
    d. Toll-free numbers, addresses, and websites for consumer reporting agencies as well as Federal Trade Commission; and
    e. A statement that the resident can obtain information from the FTC and credit reporting agencies about fraud alerts and security freezes (See Enclosure A for a sample Notice of Security Breach).
4. The notice must be made in one of the following formats:
    a. Written notice to the postal address listed in County records;
    b. Telephonic notice;
    c. Electronic notice, if the primary means of communication with the Colorado resident is by electronic means, OR the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the Federal "Electronic Signatures in Global and National Commerce Act" at 15 U.S.C 7001, *et seq.*
5. Substitute notice of either an email, a conspicuous posting of the notice on the County website, or notification via major statewide media can be made if:
    a. The cost of providing notice will exceed $250,000;
    b. The affected class of persons exceeds 250,000 Colorado residents; or
    c. The County does not have sufficient contact information to provide notice.
6. Breaches affecting 1,000 or more Colorado residents require the County to provide information to the national consumer reporting agencies of the anticipated date that the affected Colorado residents will receive notice of the breach and approximate number of affected residents. No identifying information may be shared.
7. If the security breach occurs with a third-party service provider, it is required to cooperate with the County and provide information pertaining to the breach in the most expedient time possible. The law does not include the 30-day maximum timeframe for third-party providers. Third-party providers are not required to disclose confidential business information or trade secrets.

8. If a law enforcement agency determines that giving notice to those affected by a PI breach will impede its investigation, the County may delay the notification. Once the law enforcement agency confirms that notice will no longer impede its investigation, the County is then required to provide notice no later than 30 days after receiving that confirmation.
9. If the PI identified in the security breach was encrypted, it is generally excluded from the notice provisions. However, if the encryption key, confidential process, or other means to decipher the PI was also obtained or reasonably believed to have been obtained, the notice provisions apply.
10. Offices, service areas, departments, and divisions are expressly prohibited from passing on any costs associated with providing notice to the affected Colorado residents.
11. If an investigation determines that the type of PI composed of a username or email address in combination with a password or security questions and answers that would permit access to an online account has been misused or is reasonably likely to be misused, then the applicable governmental entity shall, in addition to the notice otherwise required, adhere to the following procedure:
    a. Direct the person whose PI has been breached to promptly change their password and security questions or answer or take other steps appropriate to protect the online account with the County and all other online accounts for which the person whose PI has been breached uses the same username or email address and password or security question or answer.
    b. If login credentials of an email account are provided by the County, the notice may not be provided to that same email address. Instead, use any of the other contact methods mentioned above.
    c. These additional notices must occur in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

This Policy is hereby adopted and made effective on _____, 2021

COUNTY OF SUMMIT
STATE OF COLORADO
BY AND THROUGH ITS
BOARD OF COUNTY COMMISSIONERS

_____
Elisabeth Lawrence, Chair

ATTEST:

_____
Kathleen Neel, Clerk & Recorder

ENCLOSURE A: Sample Notice of Breach

NOTICE OF DATA SECURITY BREACH
[Date]
Provided via [Written Notice / Electronic Notice]

[Colorado Resident Name]
[Resident address if mailed, email address if electronic]

This notice is provided to you pursuant to C.R.S. 24-73-101 and C.R.S. 24-73-103, *et seq*., under the protections concerning consumer data privacy. Below, you will find information pertaining to the security breach. Please review this notice carefully as it includes information that may be useful to you in preventing or mitigating any harmful consequences resulting from the security breach. [This notice has been provided within thirty (30) days as required by law. OR This notice was delayed at the direction of [Law Enforcement Agency] and has been provided to you within thirty (30) days of notice from [Law Enforcement Agency], received by us on [DATE].]

Date of Security Breach: [DATE or estimate date or date range]

Personal Information was [acquired and/or reasonably believed to have been acquired] of the following types:

- ❑ First Name or First Initial and Last Name
- ❑ Social Security Number
- ❑ Student, Military, or Other Identification Card Number
- ❑ Driver's License Number
- ❑ Medical Information
- ❑ Health Insurance Identification Number
- ❑ Biometric Data
- ❑ Other: _____

At this time, we [are investigating / have investigated] the security breach. [We have determined that the personal information [has / has not] been misused and [is / is not] reasonably likely to be misused. [IF MISUSED, INCLUDE: As a result, you must promptly change your password and security questions or answers, if applicable, and take other steps as appropriate to protect your online account and/or all other online accounts for which you use the same username or email address and password or security question and answer, as applicable.]

If you wish to contact us about the security breach, please direct your inquiries to [NAME] at [TELEPHONE, EMAIL, AND/OR OTHER CONTACT INFORMATION].

You can get more information about fraud alerts and security freezes from the national consumer reporting agencies and/or the Federal Trade Commission. The contact information for these agencies is:

Experian P.O. Box 9530 Allen, TX 75013 1-888-397-3742 www.experian.com	Transunion P.O. Box 2000 Chester, PA, 19016 1-888-909-8872 www.transunion.com
Equifax P.O. Box 740256 Atlanta, GA, 30374 1-800-685-1111 www.equifax.com	Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC, 20580 1-877-382-4357 www.ftc.gov