ROUTT COUNTY
ADMINISTRATIVE POLICIES AND PROCEDURES
Policy Number X.XX

TITLE Personal Identifying Information (PII)	**Date of First Approval** October 30, 2018
RESPONSIBLE DEPARTMENT Information Technology	**Date Last Revised** October 19, 2021

Purpose: To provide guidance to County employees, department heads and elected officials for the proper handling of Personal Identifying Information (PII), as required by House Bill 18-1128, enacted as C.R.S. § 6-1-713, 713.5, 716 and § 24-73-101, *et. seq*. ("the Act").

The Act requires that all covered entities, which includes County governments, have in place a written policy for the destruction or proper disposal of paper and electronic documents containing PII.

The Act also sets forth requirements regarding the protection of PII, and procedures should a breach regarding PII occur.

Department(s) Affected: All.

Waiver Authority, if any: None.

I. Definitions.

A. "Biometric Data" means unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account.

B. "Departments" means all current Routt County departments and any department added after the creation of this Policy.

C. "Determination that a Security Breach Occurred" means the point in time at which there is sufficient evidence to conclude that a security breach has taken place.

D. "Routt County" or "the County" means Routt County, Colorado, acting by and through the Routt County Board of County Commissioners, and the offices of other Routt County elected officials.

E. "Encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

F. “Medical Information” means any information about a consumer's medical or mental health treatment or diagnosis by a health care professional.

G. “Notice” means:

1. written notice to the postal address listed in the records of the governmental entity;

2. telephonic notice;

3. electronic notice, if a primary means of communication by the governmental entity with a 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", 15 U.S.C. sec. 7001 *et seq.*; or

4. substitute notice, if the governmental entity required to provide notice demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be notified exceeds two hundred fifty thousand Colorado residents, or the governmental entity does not have sufficient contact information to provide notice substitute notice consists of all of the following:

    a. e-mail notice if the governmental entity has e-mail addresses for the members of the affected class of Colorado residents;
    b. conspicuous posting of the notice on the website page of the governmental entity if the governmental entity maintains one; and
    c. notification to major statewide media.

H. “Personal Identifying Information (PII)” means, 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 C.R.S. § 6-1-716 (1)(a); an employer, student, or military identification number; a financial transaction device, as defined in C.R.S. § 18-5-701 (3); or date and place of birth, mother's maiden name, criminal, medical records, financial records, and educational transcripts (see 2 C.F.R. § 200.82).

I. “Personal Information” means (A) 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 this section; (B) 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 (C) 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.

"Personal Information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

J. "Security Breach" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a governmental entity. Good faith acquisition of personal information by an employee or agent of a governmental entity for the purposes of the governmental entity is not a security breach if the personal information is not used for a purpose unrelated to the lawful government purpose or is not subject to further unauthorized disclosure.

K. "Third-Party Service Provider" means an entity that has been contracted to maintain, store, or process PII on behalf of Routt County.

L. The definitions of the Act are further hereby incorporated into this Policy to the extent not set forth above.

II. Disposal of PII.

A. It shall be the policy for all Departments that, unless otherwise required by state or federal law or regulation, when any paper or electronic documents containing PII are no longer needed to perform the Departments' essential duties or functions, the Departments shall destroy or arrange for the destruction of such paper and electronic documents within the Departments' custody or control by shredding, erasing, or otherwise modifying the PII in the paper or electronic documents so as to make the PII unreadable or indecipherable through any means.

B. The Departments shall implement inter-departmental procedures and policies which address the specific nature of their offices to ensure compliance with this Policy and the Act.

III. Protection of PII.

A. All Departments shall protect PII from unauthorized access, use, modification, disclosure, or destruction. The Departments, with assistance from the IT Department, shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII.

B. Third-Party Service Providers shall be required to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII disclosed to

the Third-Party Service Provider and reasonably designed to help protect the PII from unauthorized access, use, modification, disclosure, or destruction.

C. For purposes of this section, "reasonable security procedures and practices include the following:

1. Ensuring that there are access restrictions to documents containing PII;

2. Prohibiting the download or storage of PII on personal devices or any equipment outside of County owned devices;

3. Encrypting portable media devices so as to not allow anyone other than the intended parties to access the information;

4. Physically securing paper documents which contain PII; and

5. Requiring proper authorization from supervisors or department heads before accessing documents with PII.

IV. Internal Notification and Investigation of Suspected Security Breach.

A. Should a Department suspect that a Security Breach may have occurred, it must:

1. Immediately notify the County Manager and Information Technology Director upon becoming aware that a Security Breach may have occurred.

2. Conduct a good faith and prompt investigation to determine the likelihood that personal information has been or will be misused.

B. Unless the investigation determines that the misuse of information regarding a Colorado resident has not occurred and is not reasonably likely to occur, Routt County shall give Notice, as provided in Section V and take further action as necessary under Section VI.

C. If the investigation determines that the misuse of information regarding a Colorado resident has not occurred and is not reasonably likely to occur, Routt County need not take further action pursuant to this Policy.

V. Notice of Breach if Misuse of Information has Occurred or is Reasonably Likely to Occur.

A. Notice shall be made in the most expedient time possible and without unreasonable delay, but not later than thirty (30) 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.

B. In the event Routt County is required to provide Notice, as defined in Section G, the following information shall be provided to all affected Colorado residents:

1. The date, estimated date, or estimated date range of the security breach;

2. A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach;

3. Information that the resident can use to contact the governmental entity to inquire about the security breach;

4. The toll-free numbers, addresses, and websites for consumer reporting agencies;

5. The toll-free number, address, and website for the federal trade commission; and

6. A statement that the resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

7. Direct the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or e-mail address and password or security question or answer.

8. If the breach pertains to the log-in credentials of an email account furnished by Routt County, rather than giving notice via email, the County may comply with this section by providing notice by other methods specified under "Notice" in Section G or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or online location from which Routt County knows the resident customarily accesses the account.

9. If secured personal information was breached, and a means to decipher that secured information was also acquired or reasonably believed to have been acquired in the breach, such as a confidential process or an encryption key, that must be disclosed in the Notice as well.

10. Routt County is prohibited from charging the cost of providing such notice to individuals.

C. If any Department uses a third-party service provider to maintain computerized data that includes personal information, that Department shall require that the third-party service provider give notice to and cooperate with Routt County in the event of a security breach that compromises such computerized data. Compliance shall include notifying

Routt County of any security breach in the most expedient time and without unreasonable delay following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with Routt County information relevant to the security breach; except that such cooperation does not require the disclosure of confidential business information or trade secrets.

D. Notice pursuant to this section may be delayed if a law enforcement agency determines that such notice will impede a criminal investigation and the law enforcement agency has directed Routt County not to send notice.

VI. Further Reporting Requirements.

A. In the event Routt County is required to provide Notice, as defined in Section G, *to more* than five hundred (500) Colorado residents, it is also required to notify the Colorado Attorney General. Notification pursuant to this Section must be done as expediently as possible and without unreasonable delay, but not later than thirty (30) days after determination of a breach.

B. In the event Routt County is required to provide Notice, as defined in Section 3, *to more* than one thousand (1,000) Colorado residents, it is also required to notify all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined by the Federal "Fair Credit Reporting Act," 158 USC § 1681a(p). Routt County is not required to provide the names or other personal identifying or personal information of those subject to the breach. Notification pursuant to this Section must be done as expediently as possible and without unreasonable delay.