RESOLUTION NO. 2019- 04
BOARD OF COUNTY COMMISSIONERS
OF THE COUNTY OF RIO BLANCO
STATE OF COLORADO

A RESOLUTION OF THE BOARD OF COUNTY COMMISSIONERS OF RIO BLANCO COUNTY, COLORADO ADOPTING A POLICY FOR THE DISPOSAL OF PERSONALLY INDENTIFIABLE INFORMATION AND FOR PROPER NOTIFICATION OF A DATA BREACH

WHEREAS, Rio Blanco County ("County") regularly stores Personally Identifiable Information, herein "P.I.I.", and other sensitive information on paper, computer hard drives, and other forms of electronic media; and

WHEREAS, the Colorado legislature recently adopted House Bill 18-1128 enacted as an amendment to C.R.S. § 6-1-713, 713.5, 716 and § 24-73-101 et seq. ("The Act"), which requires governmental entities such as Rio Blanco County to adopt a written policy for the destruction or physical disposal of all paper or electronic documents containing P.I.I. after the information is no longer needed; and

WHEREAS, the Act also requires governmental entities such as Rio Blanco County to adopt a written policy in the event of a security breach involving P.I.I., the protection of P.I.I., and describing notification proceedings; and

WHEREAS, the policy adopted by this Resolution is intended to address proper disposal of P.I.I., protection of P.I.I, and establish proper notification protocols in the event of a data breach; and

WHEREAS, it would be appropriate and in the interests of the health, safety, morals, convenience, order, prosperity, and welfare of the citizens of Rio Blanco County.

NOW THEREFORE, BE IT RESOLVED AS FOLLOWS:

1) The policy regarding P.I.I. attached hereto, as Exhibit A is hereby adopted.

2) All County Department-Heads and County Elected Officials, and their employees, are directed to comply with the policy requests set forth in Exhibit A.

3) All County Department-Heads and County Elected Officials are directed to notify and instruct all of its employees concerning the P.I.I. Policy adopted by its resolution.

DULY MOVED, SECONDED, AND PASSED ON A VOTE OF 3 FOR AND 0 AGAINST, THIS 11th DAY OF February, 2019.

ATTEST:

Clerk & Recorder

The Board of County Commissioners of
Rio Blanco County, Colorado

Jeff Rector, Chairman

Si Woodruff

Gary Moyer

# Exhibit A

**Section A. DEFINITIONS**

1. **"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.

2. **"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.

3. **"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.

4. **"Medical Information"** means any information about a consumer's medical or mental health treatment or diagnosis by a health care professional.

5. **"Notice"** means:

    a. Written notice to the postal address listed in the records of the County;
    b. Telephone notice;
    c. Electronic notice, if a primary means of communication by the County 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
    d. Substitute notice if the County is required to provide notice and demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars ($250,000.00), or the affected class of persons to be notified exceeds two hundred fifty thousand (250,000) Colorado residents, or the County does not have sufficient contact information to provide notice, substitute notice consists of <u>all</u> of the following:
        i. E-mail notice if the County has e-mail addresses for the members of the affected class of Colorado residents;
        ii. Conspicuous postings of the notice on the County website page; and
        iii. Notification to major statewide media

6. **"Personal identifying information"** 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; or a financial transaction device, as defined in C.R.S. § 18-5-701 (3);

7. **"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.

    a. **"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.

8. **"Security Breach"** means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the County. The good faith acquisition of personal information by an employee or agent of the County for the purposes of the County 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.

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

## Section B. DISPOSAL OF PERSONAL IDENTIFYING INFORMATION

It shall be the policy for all County Departments that, unless otherwise required by state or federal law or regulation, when any paper or electronic documents containing personal identifying information are no longer needed by the County Departments, 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 personal identifying information in the paper or electronic documents so as to make the personal identifying information unreadable or indecipherable through any means.

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

The County shall not be responsible for ensuring destruction of personal identifying information by any Department that is required by state or federal agencies to use one or more software programs, which may include storage of data, located on servers not within the immediate control of the County.

**Section C. PROTECTION OF PERSONAL IDENTIFYING INFORMATION**

All Departments shall protect personal identifying information from unauthorized access, use, modification, disclosure, or destruction. The Departments, with assistance from the Information Technologies Department, shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information given the nature of Rio Blanco County and its size as a governmental entity.

The Departments shall require that in all contracts with third parties, which either do, or could result in, the exchange of personal identifying information, contractual terms to ensure third parties are subject to, and abiding by, the terms of this Policy.

**Section D. INTERNAL NOTIFICATION AND INVESTIGATION OF SUSPECTED SECURITY BREACH**

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

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

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

Unless the investigation determines that the misuse of information regarding a Colorado resident has not occurred and is not reasonably likely to occur, Rio Blanco County shall give Notice, as provided in Section 7 and take further action as necessary under Section 8.

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

**Section E. NOTICE OF BREACH IF MISUSE OF INFORMATION HAS OCCURRED OR IS REASONABLY LIKELY TO OCCUR**

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.

In the event Rio Blanco County is required to provide Notice, as defined in Section 3, 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.

    a. If the breach pertains to the log-in credentials of an email account furnished by Rio Blanco County, rather than giving notice via email, the County may comply with this section by providing notice in other methods specified in under "Notice" in Section 3 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 Rio Blanco County knows the resident customarily accesses the account.

8. 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.

Rio Blanco County is prohibited from charging the cost of providing such notice to individuals.

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 Rio Blanco County in the event of a security breach that compromises such computerized data. Compliance shall include notifying Rio Blanco 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 Rio Blanco County information relevant to the security breach; except that such cooperation does not require the disclosure of confidential business information or trade secrets.

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 has directed Rio Blanco County not to send notice.

**Section F. FURTHER REPORTING REQUIREMENTS**

In the event Rio Blanco County is required to provide Notice, as defined in Section A(5) , 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.

In the event Rio Blanco County is required to provide Notice, as defined in Section A(5), 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). Rio Blanco 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.

**Section G. WAIVER**

Rio Blanco County may not elicit or accepts any waiver of these notification rights or responsibilities.