

**TOWN OF RED CLIFF, COLORADO  
RESOLUTION 1, SERIES 2019**

A RESOLUTION OF THE BOARD OF TRUSTEES OF THE TOWN OF RED CLIFF, COLORADO, ADOPTING A WRITTEN POLICY REGARDING THE DISPOSAL OF DOCUMENTS CONTAINING PERSONAL IDENTIFYING INFORMATION AND REPORTING OF SECURITY BREACHES

WHEREAS, the Colorado General Assembly has adopted House Bill 18-1128 (“HB 18-1128”) concerning strengthening protections for consumer data privacy; and

WHEREAS, HB 18-1128 mandates local governments such as the Town of Red Cliff (the “Town”) to adopt policies and procedures regarding the destruction or proper disposal of documents containing personal identifying information for the protection of Colorado residents and consumers; and

WHEREAS, HB 18-1128 sets forth requirements regarding the protection of personal identifying information; and

WHEREAS, HB 18-1128 imposes certain reporting requirements in the event of a security breach with respect to personal information; and

WHEREAS, the Town desires to be in compliance with HB 18-1128 in the interests of the health, safety, and welfare of the public.

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF TRUSTEES OF THE TOWN OF RED CLIFF, COLORADO THAT:

Section 1: The foregoing recitals are incorporated by reference herein as findings and determinations of the Town Board of Trustees.

Section 2: The Town Board of Trustees hereby adopts the “Policy Regarding Disposal of Documents Containing Personal Identifying Information and Reporting of Security Breaches” attached hereto as **Exhibit A**.


Section 3. If any clause, sentence, section, or part of this Resolution, or the application thereof to any person or circumstance, shall for any reason be adjudged invalid by a court of competent jurisdiction, such judgment shall not affect the validity of the remaining portions of the Resolution and shall not affect its application to other persons or circumstances.

Section 4. This Resolution shall become effective immediately.

INTRODUCED, READ, PASSED, AND ADOPTED at a regular meeting of the Board of Trustees of the Town of Red Cliff, Colorado, held on January 15, 2019.



BOARD OF TRUSTEES OF THE  
TOWN OF RED CLIFF, COLORADO

  
\_\_\_\_\_  
Duke Gerber, Mayor Pro-tem

ATTEST

  
\_\_\_\_\_  
Barb Smith, Town Clerk

# RESOLUTION 1, SERIES 2019 - EXHIBIT A

## TOWN OF RED CLIFF, COLORADO

### POLICY REGARDING DISPOSAL OF DOCUMENTS CONTAINING PERSONAL IDENTIFYING INFORMATION AND REPORTING OF SECURITY BREACHES

#### Section 1. Purpose

The purpose of this Policy is to implement the terms of Colorado House Bill 18-1128 (the "Act") concerning strengthening protections for consumer data privacy. The Act requires that all covered entities have in place a written policy for the destruction or proper disposal of paper and electronic documents containing personal identifying information. The Act further sets forth parameters regarding notification of security breaches related to personal identifying information.

#### Section 2. Definitions

"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.

"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.

"Notice" means:

- written notice to the postal address listed in the records of the Town;
- telephonic notice;
- electronic notice, if a primary means of communication by the Town 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
- substitute notice, if the Town demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars (\$250,000), the affected class of persons to be notified exceeds two hundred fifty thousand (250,000) Colorado residents, or the Town does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:
  - e-mail notice if the Town has e-mail addresses for the members of the affected class of Colorado residents;
  - conspicuous posting of the notice on the Town's website; and
  - notification to major statewide media.

"Personal identifying information" means: (i) a social security number; (ii) a personal identification number; (iii) a password; (iv) a pass code; (v) an official state or government-issued driver's license or identification card number; (vi) a government passport number; (vii) biometric data, as defined in C.R.S. § 24-73-103(1)(a); (viii) an employer, student, or military identification number; or (ix) a financial transaction device, as defined in C.R.S. § 18-5-701(3).

"Personal information" means:

- 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 C.R.S. § 24-73-103(1)(a);
- 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
- 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.

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

"Third-party service provider" means an entity that has been contracted to maintain, store, or process personal identifying information on behalf of the Town.

"Town" means the Town of Red Cliff, Colorado, acting by and through its Board of Trustees.

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

### Section 3. DISPOSAL OF PERSONAL IDENTIFYING INFORMATION

It shall be the Town's policy 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 Town, Town personnel shall destroy or arrange for the destruction of such paper and electronic documents within its custody or control by shredding, erasing, or otherwise modifying the personal identifying information in the paper or electronic documents to make the personal identifying information unreadable or indecipherable through any means.

### Section 4. PROTECTION OF PERSONAL IDENTIFYING INFORMATION

The Town shall protect personal identifying information from unauthorized access, use, modification, disclosure, or destruction. The Town Administrator shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the size of the Town.

The Town shall require that all contracts with third-party service providers which either do, or could result in, the exchange of personal identifying information, contain contractual terms requiring such third-party

service providers to abide by the terms of the Act and this Policy. Such contractual terms shall require the third-party service provider to implement and maintain reasonable security procedures and practices that are: (i) appropriate to the nature of the personal identifying information disclosed to the third-party service provider; and (ii) reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction.

#### Section 5. NOTIFICATION OF SECURITY BREACH

Town personnel shall immediately notify the Town Administrator when they become aware that a security breach may have occurred. The Town shall conduct a prompt, good faith investigation to determine the likelihood that personal information has been or will be misused. The Town shall give Notice, as provided below, to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not 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 the Town is required to provide notice, as defined in Section 2 above, the following information shall be provided to all affected Colorado residents:

- the date, estimated date, or estimated date range of the security breach;
- a description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach;
- information that the resident can use to contact the Town to inquire about the security breach;
- the toll-free numbers, addresses, and websites for consumer reporting agencies;
- the toll-free number, address, and website for the federal trade commission; and
- a statement that the resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

If an investigation by the Town determines that personal information has been misused or is reasonably likely to be misused, then the Town shall, in addition to the notice otherwise required by above, and 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:

- 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.
- For log-in credentials of an e-mail account furnished by the Town, the Town shall not comply with this section by providing the security breach notification to that e-mail address, but may instead comply with this section by providing notice through other methods, as defined in Section 2 above,

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 the Town knows the resident customarily accesses the account.

The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired or was reasonably believed to have been acquired in the security breach.

The Town is prohibited from charging the cost of providing such notice to individuals.

In accord with Section 4, if the Town uses a third-party service provider to maintain computerized data that includes personal information, then the Town shall require that the third-party service provider give notice to and cooperate with the Town in the event of a security breach that compromises such computerized data, including notifying the Town 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 the Town information relevant to the security breach; except that such cooperation does not require the disclosure of confidential business information or trade secrets.

A waiver of these notification rights or responsibilities is void as against public policy.

#### Section 6. REPORTING OF SECURITY BREACH

If the Town must notify Colorado residents of a data breach pursuant to this Policy, and if the security breach is reasonably believed to have affected five hundred (500) Colorado residents or more, unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur, then the Town shall also provide notice of the security breach to the Colorado Attorney General 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.

If the Town is required to notify more than one thousand (1,000) Colorado residents of a security breach pursuant to this Policy, the Town shall also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal "Fair Credit Reporting Act", 15 U.S.C. sec.1681a (p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. Nothing in this Policy requires the Town to provide to the consumer reporting agency the names or other personal information of security breach notice recipients. This requirement does not apply to a person who is subject to Title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq.

A waiver of these notification rights or responsibilities is void as against public policy.

Effective: January 15, 2019