

RESOLUTION OF THE TOWN COUNCIL OF BASALT, COLORADO,
ADOPTING A PERSONAL IDENTIFYING INFORMATION POLICY

Town of Basalt, Colorado
Resolution No. 22
Series of 2020

RECITALS

- A. The Town of Basalt is subject to C.R.S. § 24-73-101, *et seq.*, which requires that: “[e]ach governmental entity in the state that maintains paper or electronic documents during the course of business that contain personal identifying information shall develop a written policy for the destruction or proper disposal of those paper and electronic documents containing personal identifying information.”
- B. The Town of Basalt wishes to adopt a policy for the purpose of safeguarding personal identifying information received by the Town of Basalt and to comply with C.R.S. § 24-73-101, *et seq.*
- C. Town Council wishes to adopt the Personal Identifying Information Policy enclosed as **Exhibit A** and repeal any conflicting policy, and believes it is in the best interests of the Town to do so.

NOW, THEREFORE, BE IT RESOLVED by the Town Council of Town of Basalt, Colorado, that:

1. Recitals. The foregoing recitals are incorporated herein as findings of the Town Council.
2. Personal Identifying Information Policy. Town Council hereby approves and adopts the Personal Identifying Information Policy enclosed as **Exhibit A** and repeals any conflicting policy that may be in effect prior to the date of this Resolution.

READ AND ADOPTED by a vote of 6 to 0 this 23rd day of June, 2020.

TOWN OF BASALT, COLORADO

By: William G. Kane
William G. Kane, Mayor

ATTEST:

By: Pamela K. Schilling
Pamela K. Schilling, Town Clerk



EXHIBIT A



BASALT

Town of Basalt

Personal Identifying Information Policy

Effective: 6/9/2020

I. Purpose

This policy intended to safeguard personal identifying information received by the Town of Basalt and to comply with C.R.S. § 24-73-101, *et seq.* requires that: “Each governmental entity in the state that maintains paper or electronic documents during the course of business that contain personal identifying information shall develop a written policy for the destruction or proper disposal of those paper and electronic documents containing personal identifying information.”

II. Policy

For purposes of this policy, “personal identifying information” (PII) includes social security numbers; personal identification numbers; passwords; pass codes; official state or government-issued driver’s license or identification card numbers; government passport numbers; biometric data (i.e. finger print or retina scan); employer, student, or military identification numbers; or financial transaction devices (i.e. credit cards, debit cards, banking cards, electronic fund transfer cards, guaranteed check cards, and financial account numbers).

In order to ensure the protection of PII, including that of Town employees, from unauthorized access, use, modification, disclosure or destruction, access to PII is limited to Human Resources personnel.

Unless otherwise required by state or federal law or regulation, when paper and electronic documents received by the Town containing PII are no longer needed for its business purposes, the Town will destroy or arrange for the destruction of the documents in its custody by shredding, erasing, or otherwise modifying the PII in the documents to make the information unreadable or indecipherable through any means.

The Town will take no more than 30 days to provide Employees notice of a security breach that results in or is likely to result in the misuse of PII when the breach involves a Colorado resident's first name or first initial and last name in combination with: the individual’s social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data; username or email address, in combination with a password or security questions and answers, that would permit access to an online account; or an 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, when any of these data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable.