PERSONAL IDENTIFYING INFORMATION POLICY

1. Purpose. The purpose of this Personal Identifying Information Policy ("Policy") is to facilitate compliance with C.R.S. §§24-73-101 *et seq.* (the "Act").

2. Definitions. The following definitions shall apply to this Policy, unless otherwise provided in the Act, in which case the Act shall control:

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. "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; an employer, student, or military identification number; or a financial transaction device as defined in C.R.S. § 18-5-701(3).

c. "Personal information" means:

i. 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.
ii. 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
iii. 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

d. "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.

3. Disposal Policy. Unless otherwise required by state or federal law or regulation, when paper or electronic documents containing personal identifying information are no longer needed, the Town 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.

4. Security Procedures. The Town shall protect personal identifying information from unauthorized access, use, modification, disclosure or destruction. To effectuate the foregoing, unless otherwise required by law, the Town shall:

a. Keep all records containing personal identifying information in a secure location to the extent practicable;
b. Limit access to personal identifying information to Town employees or to agents that require access in their official capacities and require such employees and agents to maintain the confidentiality of the personal identifying information;
c. Prohibit disclosure of personal identifying information to third parties absent a legitimate Town purpose;
d. Require third-party service providers to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information provided to such provider and reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure or destruction;
e. Cooperate with law enforcement in the event of a security breach; and
f. Endeavor to promptly restore the integrity of the Town's computer systems in the event of a security breach.

5. Notification of Security Breach. When the Town becomes aware that a security breach may have occurred, the Town shall comply with the notification procedures set forth in C.R.S. § 24-703-103, as amended.

6. State or Federal Law Regulations. Pursuant to C.R.S. §24-73-101(2), Town records regulated by state or federal law establishing procedures for disposal of personal identifying information shall be deemed to be in compliance with this Policy and the Act.