TOWN OF MEAD, COLORADO
RESOLUTION NO. 94-R-2020

A RESOLUTION OF THE TOWN OF MEAD, COLORADO, ADOPTING THE TOWN OF MEAD DATA BREACH PROTOCOL AND PERSONAL DATA PROTECTION POLICY

WHEREAS, the Town of Mead, in its ordinary course of governmental operations, maintains and utilizes a limited amount of personal identifying information and/or computerized data that include personal identifying information; and

WHEREAS, the Colorado legislature recently enacted C.R.S. §§ 24-73-101, et seq., which requires local governments to implement new data protection policies to prevent unauthorized use or disclosure of certain kinds of personal information within a local government's custody or control; and

WHEREAS, to comply with the data protection requirements set forth in state law, the Town desires to implement the Data Breach Protocol and Personal Data Protection Policy, attached hereto as **Exhibit A** and incorporated herein by this reference ("Policy"); and

WHEREAS, the Board desires to adopt the Policy and finds and determines that the Policy is reasonably designed to reasonably protect the personal information in the custody and control of the Town.

NOW THEREFORE, BE IT RESOLVED by the Board of Trustees of the Town of Mead, Weld County, Colorado, that:

Section 1. The foregoing recitals and findings are incorporated herein as findings and conclusions of the Board of Trustees.

Section 2. The Board of Trustees hereby adopts the Policy in the form attached hereto as **Exhibit A**. The Board reserves the right to amend the Policy from time to time. Any amendments to the Policy shall be memorialized by adoption of a resolution of the Board considered at a regular or special meeting of the Board.

Section 3. **Effective Date.** This Resolution shall be effective immediately upon adoption.

Section 4. **Repealer.** All resolutions, or parts thereof, in conflict with this Resolution are hereby repealed, provided that such repealer shall not repeal the repealer clauses of such resolution nor revive any resolution thereby.

Section 5. **Certification.** The Town Clerk shall certify to the passage of this Resolution and make not less than one copy of the adopted resolution available for inspection by the public during regular business hours.

INTRODUCED, READ, PASSED, AND ADOPTED THIS 30TH DAY OF NOVEMBER, 2020.

ATTEST:

By: _____
Mary E. Strutt, MMC, Town Clerk

TOWN OF MEAD SEAL WELD COUNTY, COLORADO

TOWN OF MEAD

By: _____
Colleen G. Whitlow, Mayor

EXHIBIT A

TOWN OF MEAD DATA BREACH PROTOCOL AND PERSONAL DATA PROTECTION POLICY

[Attached.]

Town of Mead

Data Breach Protocol and Personal Data Protection Policy

I. Purpose

The Colorado General Assembly enacted C.R.S. §§ 24-73-101, *et seq.*, which requires the Town to implement new data protection policies to prevent unauthorized use or disclosure of certain kinds of personal information within the Town's custody or control. The purpose of this Data Breach Protocol and Personal Data Protection Policy ("Policy") is to protect Personal Information and Personal Identifying Information, as defined herein, and provide for the timely destruction of same.

A Security Breach, as defined herein, can be caused by any number of events, such as loss or theft of a device containing data, loss or theft of paperwork, burglary, equipment failure, malicious attacks using spyware or ransomware, or other unauthorized access, acquisition or use. This Policy seeks to prevent Security Breaches and mitigate potential consequences such as identity theft or fraud, loss of confidentiality of personal data, financial loss, damage to reputation to affected individuals, damage to relationships with citizens, and loss or damage to data.

II. Definitions

For purposes of this Policy, the terms below have the meaning given to them in C.R.S. §§ 24-73-101, *et seq.*, and 18-5-701(3), both as amended. The following definitions are provided for convenience. In the event there is a conflict between a definition contained in this Policy and the corresponding definition in the statute, the statute controls.

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. "Employee(s)" or "Town employee(s)" means Town employees, agents, contractors, or other individuals with lawful access to Town data, including Personal Information and Personal Identifying Information.

3. "Financial Transaction Device" means any instrument or device whether known as a credit card, banking card, debit card, electronic fund transfer card, or guaranteed check card, account number representing a financial account or affecting the financial interest, standing, or obligation of or to

III. Reporting a Data Breach

Any employee who knows or suspects that a data breach may have occurred should notify the Town Clerk and the Information Technology Department (including contractors, if applicable) ("IT Department") immediately utilizing the attached **Notification of Security Breach Form.** After conducting the initial investigation and determining if one or more systems may have been breached, the IT Department should notify the Town Manager.

IV. Containing a Data Breach

Employees that know or suspect that a data breach may have occurred should take the following measures to contain the breach after reporting in accordance with Section III.

a. Disconnect internet
b. Disable remote access
c. Maintain firewall settings
d. Install pending security updates or patches
e. Change passwords

V. Investigation and Notification of a Security Breach

1. Investigation. As soon as the Town becomes aware that a Security Breach may have occurred, the Town shall, through its IT Department, conduct a good faith and prompt investigation to determine if any Personal Information was misused or is reasonably likely to be misused. Depending on the severity of the Security Breach, the Town may contract with a data security consultant to assist in the investigation.

2. Notice. As expediently as possible and without unreasonable delay, and no later than thirty days from the determination that a Security Breach has 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, the Town shall provide all affected Colorado residents with notice of the Security Breach, unless the Town's investigation determines that no Personal Information was misused, and misuse is reasonably likely not to occur.
    a. Any notice provided by the Town will contain the information required by C.R.S. § 24-73-103(2)(b). If the Security Breach includes email account log-in credentials, the Town will provide notice to affected Colorado residents by an uncompromised means of communication defined in C.R.S. § 24-73-103(1)(f).
    b. In addition to providing the required notice, the Town shall direct

compliance with this Policy and should conduct training as needed.

3. The Town shall keep all records containing Personal Identifying Information and Personal Information in a secure location, either physically at municipal offices or in a password- protected or encrypted electronic format.

4. The Town shall limit access to systems or files containing Personal Identifying Information to employees that require access to Personal Identifying Information in their official capacities. Employees with access to Personal Identifying Information must respect the confidentiality of such information, and refrain from all careless or negligent conduct that might lead to unauthorized access, use, modification, disclosure, or destruction of Personal Identifying Information.

5. Employees are prohibited from sharing or disclosing Personal Identifying Information to any party without their manager's or supervisor's prior written consent. The Town shall only give approval for disclosure or sharing of Personal Identifying Information when necessary to conduct Town business.

6. The Town shall require that if Personal Identifying Information is disclosed to a third-party service provider in the course of the Town's business, the third-party service provider will implement and maintain reasonable security procedures and practices that are appropriate to the nature of the Personal Identifying Information disclosed by the Town and reasonably designed to help protect the Personal Identifying Information from unauthorized access, use, modification, disclosure or destruction.

7. In the event of a Security Breach, the Town shall cooperate with law enforcement and work promptly to restore the integrity of the Town computerized systems containing Personal Identifying Information and/or Personal Information and comply with Section V.

8. The IT Department is responsible for identifying data breach risks, recommending appropriate controls to prevent data breaches, implementing those controls, and continually evaluating the controls' performance.

9. No employee shall transport any hard copy files containing Personal Identifying Information outside of municipal offices unless such files remain in the employee's custody at all times until such files are returned to Town offices or destroyed in accordance with Section VII.

MEAD
COLORADO

Notification of Security Breach Form

1. **Date and time of breach:**

   _____

2. **Date and time of discovery of breach:**

   _____

3. **Where did the breach happen?**

   _____
   _____

4. **Name of person reporting the breach:** _____

   Organization or Department: _____

5. **Name of person/organization responsible for the breach (if known):**

   _____
   _____

6. **Type of Data Breach (i.e. theft, illegal access, virus, etc.):**

   _____
   _____
   _____

7. **What network resources were breached? (routers, firewalls, servers, etc?)**

   _____
   _____
   _____

15. Controls implemented to prevent future breaches:

_____
_____
_____

16. Other Comments:

_____
_____
_____

Please attach any support documentation, if necessary, to fully answer the above questions.

Name: _____ **Date:** _____

Reported to: _____ **Date:** _____