Town of Carbondale
February 7, 2018
Data Breach Plan

I. Purpose:

The purpose of this plan is to prevent a serious disruption of operations, loss of funds, or damage to reputation by providing an immediate and effective response to any unexpected event involving the unauthorized access of computer information systems, network, or databases. The plan also encompasses confidential hardcopy files such as claim files, personnel and financial records, and information contained in portable media such as flash drives, or contained in transportable equipment such as laptops or tablets.

II. Definition of a Data Breach:

For the purposes of this plan, a "data breach" is defined as the unauthorized acquisition of data that compromises the security, confidentiality, or integrity of member, organization or employee information maintained by Town of Carbondale.

III. Possible Perpetrators:

Persons who could breach our data include:

- Former employees
- Current employees
- Vendors
- Hackers
- Members
- Visitors

IV. Responsibilities:

1. All employees are responsible for following this plan, keeping data secure and reporting any potential data breaches.
2. Managers are responsible for implementing security controls in their respective departments and supervising employees to ensure security policies are adhered to.
3. The Town's Contract IT vendor is responsible for identifying data breach risks, recommending appropriate controls to prevent data breaches, implementing those controls, and continually evaluating the controls to ensure they work. They are also responsible for investigating and mitigating any data breaches that may occur.

V. Risk Classifications of Data Breaches:

The following classification system will be used to identify the risk associated with the unauthorized access of data.

High Risk: A breach of this information may result in high costs to the Town of Carbondale; significantly harm our reputation with members and other organizations; or seriously impact employees or other individuals.

Medium Risk: A breach of this data may result in moderate costs to the Town of Carbondale, could result in some damage of reputation if not handled promptly and effectively; or could impact employees or individuals.

Low Risk: A breach of this information is easily controlled and should not result in significant costs to the Town of Carbondale; should not harm our reputation; and should not require notification of members, employees or others.

VI. Database Risk Classification by Department:

The following data may be at risk of being breached:

	Risk Classification
Finance Department:	
1. Personnel records	Medium
2. Social security numbers for employees	High
3. Payroll information	High
4. Performance reviews	Medium
5. Credit card information	High
6. Bank accounts	High
7. Investment accounts	High
8. Human resource files	High
9. Other financial records containing confidential information	High
Contract IT Provider	
1. Employee user names and passwords	High
2. Outlook email database	Medium
3. Admin user names and passwords	High
4. Databases (Finance, etc.)	High

Other Departments:

Public Works: Website user names/passwords	Low
Police Department:	High
Parks & Recreation Department:	Low
Town Clerk: Election Data	Medium
Utilities: Water/Sewer Systems	Medium

.

VII. Protection of Data:

1. To protect the integrity of data, no employee shall transport any hard copy files containing high or medium risk data outside of Town offices.
2. No employee shall copy or place any high risk data onto any flash drive, Google drive or cloud storage.
3. Laptops or tablets shall not be left in vehicles or placed in checked airline baggage.
4. Users are required to have complex passwords expiring every three months.
5. Screen savers implemented to lock after 10 minutes requiring logging back into desktop.
6. Sensitive data shall not reside on or in any personal email account or electronic device.
7. Employees will not share passwords and logins with anyone except IT contractor and Management.

VIII. Reporting a Data Breach:

Any employee who knows or suspects that a data breach may have occurred should notify their supervisor, Town Manager and IT contractor immediately. After conducting the initial investigation and determining if one or more systems may have been breached, IT contractor should notify the department heads of departments that are affected. The attached Data Breach Incident Report Form should be used to document information.

IX. Containing and Investigating a Data Breach:

After a breach is discovered, IT Contractor and other applicable employees will take immediate steps to limit the breach. These steps should include:

- Immediately containing the breach by stopping an unauthorized practice, recovering records, revoking access, or correcting physical security. Care should be taken so not to destroy any evidence.
- Contacting the appropriate managers and vendors.

- Determine where and how the breach occurred:
    - Identify the source of the compromise and the timeframe involved.
    - Document the chronology of the event.
    - Document how the breach was discovered.
    - Review the network to identify all compromised or affected systems.
    - Document all internet protocol addresses, operating systems, domain systems names and other pertinent system information.
    - Use the attached Data Breach Incident Report Form to document the breach.
- Determine the type of information that was lost or compromised, including but not limited to:
    - Names, addresses, social security numbers, account numbers, cardholder names, medical and health information, financial records, etc.
    - Determine if an intruder has exported or deleted any personal information.
- Secure and protect the integrity of the evidence and ensure that any systems affected by a breach are only accessible to internal investigators and law enforcement.
- Take measures to contain and control the incident to prevent further unauthorized access to or use of sensitive information. Consider shutting down related applications or third-party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls:
    - Change applicable passwords for users that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.
    - Do not alter the compromised system.
    - Do not turn off the authorized machine. Isolate the system from the network (i.e. unplug cable).
    - Change the wireless network SSID on the access point and other authorized devices that may be using our wireless network.
- Preserve all system and audit logs and evidence for law enforcement in the event of a criminal investigation.
- If the breach occurred at a third-party location, work with the appropriate parties to determine the extent of the breach.
- Notify law enforcement if there is suspected theft or other criminal activity.
- A forensic investigation expert may be hired to conduct an investigation of the breach if deemed necessary.
- Monitor systems and network for signs of continued intruder access.

X. Notification of Individuals and Entities:

Once the incident is investigated and the extent of the compromise determined, notification may take place in order to mitigate harm to an employee, individual or entity whose personal information has been inappropriately collected, used, or disclosed. Factors to consider for notification include:

- Any state or federal law that requires notice (see attached Colorado law)
- Contractual obligation that requires notification
- Risk of identity theft or fraud
- Risk of physical harm
- Risk of damage to reputation
- Risk of loss of business

XI. When to Notify:

Notification of individuals and members affected by the breach should occur as soon as possible after the breach. However, notification may be delayed if law enforcement authorities who are brought into the investigation recommend delaying the notification so as not to impede a criminal investigation.

XII. How to Notify:

The Management Team will determine if notification is needed, who will notify affected parties and how the notification will take place. The method of notification to those affected may be done directly by telephone, letter, in person, or email as long as:

- The identities of individuals and organizations are known.
- Current contact information is available.
- Individuals and organizations affected need detailed information in order to protect themselves from possible harm arising from the breach.

Indirect notification, such as via the Carbondale website, may be considered if individual notification is not practical.

XIII. Information to include in the Notification:

Information in the notification may include the following:

- Date or time period that the breach occurred
- A general description of how the breach occurred
- Description of the information involved in the breach (name, credit card numbers, social security numbers, medical records, etc.)
- Description of the steps taken to reduce the risk of harm
- Plans to prevent future breaches
- Information on how individuals or entities can prevent further harm
- Contact information for questions

XIV. Others to Contact:

The following organizations and individuals may be notified of the breach if deemed appropriate.

- Carbondale citizens
- Carbondale employees
- Law enforcement
- Excess insurers
- Banks and other financial institutions
- Credit card companies
- Vendors
- Government agencies
- Others as deemed appropriate

XV. Employee Training:

The IT Contractor will train all employees on the prevention of data breaches and their responsibilities in the event of a data breach as necessary.

XVI. Follow Up and Review:

Once the data breach has been mitigated, appropriate notifications provided, and the investigation concluded, a post mortem analysis will take place to determine the effectiveness of the data breach plan. Among the items to consider include:

- How did the data breach occur?
- Have controls been implemented to prevent a future data breach?
- Was the data breach plan followed?
- Are plan revisions needed?
- What lessons did we learn?
- What can we do better if it happens again?

After the critique is completed, methods to mitigate any risks will be identified and measures to prevent future data breaches will be implemented.

Colorado State Security Breach Laws:

CRS 6-1-716

Definition of Personal Information: A Colorado's 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 other method rendering the name or the elements unreadable or unusable.

a) Social security number;
b) Driver's license number or identification card number; and
c) Account number or credit card number, in conjunction with any required security code, access code, or password that would permit access to a resident's financial account.

Summary: An individual or a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or the commercial entity shall give notice as soon as possible to the affected Colorado resident 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, 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.

Town of Carbondale

Data Breach Incident Report 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 if other than ____: _____
5. **Name of person/organization responsible for the breach (if known):**
   _____
   _____
6. **How did they do it?**
   _____
   _____
   _____
7. **Type of Data Breach (i.e. theft, illegal access, virus, etc.):**
   _____
   _____
   _____
8. **What network resources were breached? (routers, firewalls, servers, etc?)**
   _____
   _____
   _____
9. **Specific data compromised:**
   _____
   _____
   _____
   _____
10. **How did the breach happen?**
    _____
    _____
    _____
    _____

11. Corrective action taken to control the breach:

_____
_____
_____
_____
_____

12. Steps taken to preserve evidence:

_____
_____

13. ____ employees who were notified of the breach:

_____
_____
_____

14. Outside organizations notified of the breach:

_____
_____
_____

15. Was law enforcement notified? Yes__ No__

a. **Time and date of notification:**

_____

b. **Name of officer/department?**

_____
_____

16. Controls implemented to prevent future breaches:

_____
_____
_____

17. Other Comments:

_____
_____
_____

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

Name: _____ **Date:** _____

Reported to:_____ **Date:**_____