Town of Middlefield
Otsego County, New York
Data Breach Response Policy

1.0 Purpose

The purpose of the policy is to establish goals for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metric as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

- **Background**

This policy mandates that any individual who suspects that a theft, breach or exposure of Town of Middlefield protected data or sensitive data has occurred must immediately provide a description of what occurred via e-mail to <townofmiddlefieldsupervisor@gmail.com>, or by calling the Town Clerk at 607-547-5093, This e-mail address and phone number are monitored by the Town of Middlefield's Information Technology (IT) Director. The town will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the IT Director will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all persons who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of Town of Middlefield employees, officials, and contractors.

3.0 Procedure upon Confirmed theft, data breach or exposure of Town of Middlefield Protected data or Town of Middlefield Sensitive data:

As soon as a theft, data breach or exposure containing Town of Middlefield Protected data or Sensitive data is identified, the process of removing all access to that resource will begin.

The Town Supervisor will chair an incident response team to handle the breach or exposure.

The team will include:

- IT director
- Finance/accounting (if applicable)
- Town attorney
- Town Clerk
- Highway Department (if HIghway employee data is affected)
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Supervisor.

3.1 Work with Forensic Investigators

As provided by Town of Middlefield cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

3.2 Develop a communication plan.

The response team will work with Town of Middlefield clerk, attorney and board members to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

4.0 Ownership and Responsibilities

Roles & Responsibilities:

Sponsors - Sponsors are those members of the Town of Middlefield government that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Town of Middlefield official in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

Information Technology Director is that official of the Town of Middlefield, designated by the Town Board, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

Users include virtually all members and employees of the Town of Middlefield government to the extent they have authorized access to information resources, and may include elected officials, staff, contractors, consultants, interns, temporary employees and volunteers.

5.0 Enforcement

Any Town of Middlefield personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

6.0 Definitions

Encryption or encrypted data – Information that is encoded in a way that makes it impossible to read without access to a secret key or password that enables you to decrypt it.

Plain text – Unencrypted data, readable by anyone with access to the file containing the data.

Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

Personally Identifiable Information (PII) - Any data that could potentially identify a specific

individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

Protected data - See PII and PHI

Information Resource - The data and information assets of an organization, department or unit.

Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

Town of Middlefield Data Breach Policy
Revised February 3, 2022