WRITTEN INFORMATION SECURITY PROGRAM

PREPARED FOR:

Town of Colrain MA

Table of Contents

1.0 Policy Statement

The Town of Colrain MA Written Information Security Program ("WISP") is intended as a set of guidelines and policies designed to safeguard all confidential and restricted data maintained at Town of Colrain MA.

2.0 Overview & Purpose

The WISP was implemented to document the measures in place by Town of Colrain MA to ensure they maintain best practices for data protection and security.

Town of Colrain MA is committed to protecting the confidentiality of all sensitive data that it maintains.

The purposes of this document are to:

- Establish a comprehensive information security program for Town of Colrain MA with policies designed to safeguard sensitive data that is maintained by Town of Colrain MA, in compliance with information technology best practices.
- Establish employee responsibilities in safeguarding data according to its classification level; and
- Establish administrative, technical, and physical safeguards to ensure the security of sensitive data.

3.0 Scope

This Program applies to all Town of Colrain employees, elected and appointed officials. This program also applies to certain contracted third-party vendors (see section 4.6 for further information). The data covered by this Program includes any information stored, accessed, or collected by the Town or its contractors. The WISP is not intended to supersede any Town policy that contains more specific requirements for safeguarding certain types of data. If such policy exists and is in conflict with the requirements of the WISP, the other policy takes precedence.

3.1 Definitions

Data

For the purposes of this document, data refers to information stored, accessed, or collected that resides on Town of Colrain MA's Information systems. This includes both systems physically located at Town of Colrain MA's locations and data located with cloud vendors contracted by Town of Colrain MA.

Data Systems

Any device used to store and/or access data. This includes but is not limited to smart phones, tablets, computers, and servers.

Physical Location

Any physical location that Town of Colrain MA maintains. This includes but is not limited to owned or rented office space, warehouse space, employee's home office space, and town vehicles.

Cloud

Any service that hosts data on servers not physically owned by Town of Colrain MA.

Data Custodian

A data custodian is responsible for maintaining the technology infrastructure that supports access to the data, safe custody, transport, and storage of the data and provide technical support for its use. A data custodian is also responsible for implementation of the business rules established by the data steward.

Data Steward(s)

A data steward is responsible for the data content and development of associated business rules, including authorizing access to the data.

Site Administrator(s)

A Site Administrator is a person who is responsible for the physical access to Town of Colrain MA's equipment physically located at their locations.

Incident Response Team

The employees who are responsible for coordinating the response to any data breach incident. This team will include NEIT and a minimum of two Town of Colrain MA employees, one to serve as primary and one as a backup in the event the primary is unavailable.

Personal Information

Personal Information ("PI"), as defined by Massachusetts law (201 CMR 17.00), is the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password.
- For the purposes of this Program, PI also includes passport number, alien registration number or other government-issued identification number.

3.2 Data Classification

All data covered by this policy will be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level.

Confidential

Confidential data refers to any data where unauthorized access, use, alteration, or disclosure of this data could present a significant level of legal or financial risk to Town of Colrain MA. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration, or disclosure.

Confidential data may also include data that is protected by federal or state laws or regulations.

Restricted

Restricted data refers to all other town data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operations or reputation of Town of Colrain MA. Any non-public data that is not explicitly designated as Confidential should be treated as Restricted data.

This data also includes, but is not limited to, citizen information, intellectual property (proprietary research, etc.), financial and investment records, employee salary information, or information related to legal or disciplinary matters.

Restricted data should be limited to access by individuals who are employed by Town of Colrain MA and who have legitimate reasons for accessing such data. A reasonable level of security should be applied to this classification to ensure the privacy and integrity of this data.

Public (or Unrestricted)

Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to Town of Colrain MA. Any data that is not classified as Confidential or Restricted should be considered Public data.

4.0 Policy

4.1 Responsibilities

All data at Town of Colrain MA is assigned a data steward by Town officials. Data Steward(s) are defined in section 6.0 of this document. Data stewards are responsible for approval of all requests for access to such data. The data steward may appoint a designee to serve in their place.

Northeast IT Systems, Inc (NEIT), is contracted by Town of Colrain MA and in their capacity, they serve as the data custodians for data stored on Town of Colrain MA's Computer Systems. NEIT is responsible for the administration of the data systems. The Data stewards maintain the responsibility to inform NEIT of changes to employee's and contractor's roles or need for access to data. NEIT's responsibilities are limited to making data access adjustments as requested by the data stewards. The appropriate data stewards must be identified and made known to NEIT.

Data stewards will inform NEIT staff about an employee's change of status or termination as soon as is practical, whenever possible, if the employee is being dismissed, this should occur before the employee's departure date from Town of Colrain MA. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to Town of Colrain MA's data.

Town of Colrain MA will alert NEIT at the conclusion of a contract for individuals that are not considered Town of Colrain MA employees in order to terminate access to their Town of Colrain MA accounts.

Town of Colrain MA oversees maintaining, updating, and implementing this Program and has overall responsibility for this Program. This document should be reviewed at least annually with that review document in section 7.0.

4.2 Identification and Assessment of Risks to Town of Colrain MA's Data

Town of Colrain MA recognizes that it has both internal and external risks to the privacy and integrity of Town of Colrain MA's information. These risks include, but are not limited to:

- Unauthorized access of Confidential data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of Confidential data by employees
- Unauthorized requests for Confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential data through third parties

Town of Colrain MA recognizes that this may not be a complete list of the risks associated with the protection of Confidential data. Since technology growth is not static, new risks are created regularly. Accordingly, NEIT will actively participate and monitor technology industry groups for identification and mitigation of new risks.

Town of Colrain MA believes the town's current safeguards are reasonable.

Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

4.3 Policies for Safeguarding Confidential Data

To protect Town of Colrain MA data classified as Confidential, the following policies and procedures have been developed that relate to access, storage, transportation and destruction of records.

Access & Storage

Only those employees or authorized third parties requiring access to Confidential data in the regular course of their duties are granted access to this data, including both physical and electronic records.

To the extent possible, all electronic records containing Confidential data should only be stored in a safe and secure location provided by Town of Colrain MA.

Confidential data must not be stored on cloud-based storage solutions that are not approved by Town of Colrain MA. and vetted by NEIT for adequate security.

Employee's are strongly discouraged from storing Confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). However, if it is necessary to transport Confidential data electronically, the mobile device containing the data must be encrypted and the device is considered property of Town of Colrain MA until such time that the confidential data can be verified as being removed.

To the extent possible, paper records containing Confidential data should be kept in locked files or other secured areas when not in use.

Servers are to be maintained in secure, limited access locations maintained by the Data Stewards. It is preferred that servers are either in a dedicated locked room or a locked server rack.

Upon termination of employment or relationship with Town of Colrain MA, electronic and physical access to documents, systems or other network resources containing Confidential data is immediately terminated.

Employees are required to surrender any data systems or keys to limited access areas that they may possess upon request of management.

Transporting Confidential Data

Employees of Town of Colrain MA may not remove records containing Confidential data from Town of Colrain MA's locations without approval from management.

In rare cases where it is approved to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing Confidential data to be left unattended in any unsecure location.

- When there is a legitimate need to provide records containing Confidential data to a third party outside Town of Colrain MA, electronic records shall be password-protected and encrypted, and paper records shall be marked confidential and securely sealed.

Destruction of Confidential Data

- Records containing Confidential data must be destroyed once they are no longer needed for business purposes, unless state or federal regulations require maintaining these records for a prescribed period of time.
- Paper and electronic records containing Confidential data must be destroyed in a manner that prevents recovery of the data.
- All electronic data must be destroyed in compliance with the DoD 5220.22-M standard.

4.4Policies for Safeguarding Restricted Data

- Access to Restricted Data should be limited to those who have a legitimate business need for the data.
- Restricted Data can only be stored in locations approved by Town of Colrain MA.
- Documents containing Restricted Data should not be posted publicly.

4.5 Password Requirements

In order to protect Town of Colrain MA data, all employees must select unique passwords following these guidelines:

- Has at least 8 characters
- Contains a combination of at least three of the four character types: uppercase and lowercase letters, numbers, and special characters (e.g., @ $ # !)

Employees must protect the privacy of their passwords. Passwords must not be shared with others. If an account or password is suspected to have been compromised, all passwords should be changed immediately, and the incident reported to Town of Colrain MA management. It is the responsibility of Town of Colrain MA management to report the incident to NEIT for incident response.

4.6 Third-Party Vendor Agreements Concerning Protection of Personal Information

Town of Colrain MA exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards. The management team at Town of Colrain MA are responsible for identifying those third parties providing services to Town of Colrain MA. NEIT will review any requests for third party access to data systems and provide recommendations on best security practices to provide access. All relevant contracts with these third parties are reviewed and approved by Town of Colrain MA to ensure the contracts contain the necessary language regarding safeguarding data. It is the responsibility of Town of Colrain MA to confirm that the third parties are required to maintain appropriate security measures consistent with this Program.

4.7 Data system safeguards

Northeast IT Systems (NEIT) staff monitor and assess safeguards on an ongoing basis to determine when enhancements are required. Town of Colrain MA has implemented the following to combat external risk and secure the systems containing Confidential Data:

Secure user authentication protocols:

- Unique passwords are required for all user accounts; each employee receives an individual user account.
- Computer access passwords are disabled upon an employee's termination.
- User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.
- Secure access control measures:
- Access to specific files or databases containing Confidential Data is limited to those employees who require such access in the normal course of their duties.
- Operating system patches and security updates are installed to all computers on a regular basis.
- Antivirus and anti-malware software is installed and kept updated on all workstations.

4.8 Employee Training

All employees are required to familiarize themselves with this Program.

Additionally, any users who are the victims of a phishing attack will be required to complete a phishing education program within 2 weeks after the issue has been identified, regardless if they have already completed the training. If a user fails to complete the training within 2 weeks, his or her remote access to Town of Colrain MA resources may be disabled. It is the responsibility of the user's direct supervisor to ensure this training is completed.

Periodically NEIT may elect to run email campaigns to test Town of Colrain MA employee's response to simulated malicious emails. Town of Colrain MA Management will not be aware of when these campaigns are run and will not be exempted from the campaigns. The results of the campaign will be shared with management. Access to training will be provided at the conclusion of the campaign. The exact manner of the training will be dependent on the results of the tests and determined by both NEIT and Town of Colrain MA management.

4.9 Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of data, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the Town of Colrain MA management. Town of Colrain MA will contact NEIT who will take actions necessary to mitigate the data exposure. NEIT will be responsible for the technical response to the breach, Town of Colrain MA is responsible for any reporting that may be required of such a breach as well as any disciplinary action to be taken as a result. NEIT will provide Town of Colrain MA with a report detailing the actions taken in response to the breach. Town of Colrain MA will identify an incident response team consisting of a minimum of two employees, a primary contact and a backup contact, who NEIT will work directly with during the response to the incident.

5.0 Enforcement

Any employee or official who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Confidential or Restricted Data without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, up to and including termination of employment or removal from office.

6.0 Definition of Key People

Position	Name	Email	Phone
Data Steward	Kevin Fox	bos@colrain-ma.net	413-624-3454
Data Custodian	Northeast IT Systems	helpdesk@northeastit.net	413-736-6348
Incident Response Primary	Kevin Fox	bos@colrain-ma.gov	413-624-3454
Incident Response Secondary	Paula Harrison	Treasurer@colrain-ma.gov	413-624-3454
Site Administrator	Kevin Fox	bos@colrain-ma.gov	413-624-3454

7.0 Revision History

Date	Revision
10/2/2023	First Draft

10/17/2023	Second Draft
11/1/2023	Third Draft
11/10/2023	Proposed Final draft.
11/14/2023	Adopted by Select Board