DEPARTMENT OF INFORMATION TECHNOLOGY

Cindy Knox
(978) 772-8252

Town of Ayer, Massachusetts
1 Main Street – Ayer, MA

TOWN OF AYER
COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM

Approved by the Ayer Board of Selectmen April 19, 2016
Approved by the Ayer Board of Selectmen February 20, 2018

Reviewed and updated on February 14, 2018

I. OBJECTIVE:

The Town of Ayer's objective, in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth of Massachusetts, and to comply with obligations under 201 CMR 17.00.

This WISP sets forth the Town's procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of the Commonwealth of Massachusetts. For purposes of this WISP, *"personal information" means a resident's first name and last name or first initial and last name* ***in combination with any one or more of the following data elements that relate to such resident:*** *(a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided,* however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

For purposes of this WISP, all documents and other data, whether in electronic or "paper" form, shall be presumed to contain "personal information" unless otherwise clearly established and labeled.

II. PURPOSE:

The purpose of this WISP is to:

a) Ensure the security and confidentiality of personal information;
b) Protect against any anticipated threats or hazards to the security or integrity of such information; and
c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE:

This WISP covers all officials and employees, including temporary or contract employees who have access to personal information, in the Town of Ayer.

In formulating and implementing the Plan, the Town of Ayer has and will continue to:

(a) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;

(b) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

(c) Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;

(d) Design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00;

(e) Regularly monitor the effectiveness of those safeguards.

(f) Due to the unique legal and security requirements of the Ayer Police Department, the Ayer Police Department is exempt from this Policy.

IV. INFORMATION TECHNOLOGY DIRECTOR:

The Town's Information Technology Director is charged with the implementation, supervision and maintenance of the WISP.

Additionally, IT Director will be responsible for:

a. Training employees;
b. Regular testing of the WISP's safeguards;
c. Evaluating the ability of each of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, consistent with 201 CMR 17.00; and requiring such third party service providers by contract to implement and maintain appropriate security measures;
d. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in legal requirements or the Town's practices that may implicate the security or integrity of records containing personal information;
e. Conducting mandatory monthly training sessions for all employees who use the Town's computers. All attendees at these on-line training sessions are required to certify their attendance at the training, and their familiarity with the Town's requirements for ensuring the protection of personal information;
f. Review the security practices of all vendors who provide off-site data storage to the Town and those who accept payments on the Town's behalf.

V. INTERNAL RISKS:

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, (where necessary) the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately. To the extent that any of these measures require a phase-in period, such phase-in must be completed on or before June 30, 2016:

Internal Threats

- A copy of the WISP will be distributed to each employee who shall, upon receipt of the WISP, acknowledge in writing that he/she has received a copy of the WISP.
- There will be training of employees on the detailed provisions of the WISP.
- Access to records containing personal information is limited to those persons who are reasonably required to know such information in order to accomplish legitimate business or to enable compliance with other state or federal regulations.
- Electronic access to user identification after multiple unsuccessful attempts (three attempts within fifteen minutes) to gain access will be blocked. Logging in may be retried in thirty minutes.
- Prior to the end of employment or service with the Town, terminated or separated officials or employees must return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
- A terminated employee, or Special Town employee's physical and electronic access to personal information will be immediately blocked. Terminated employees shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the Town's premises or information. Remote electronic access to personal information will be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.
- Current employees' passwords will be changed every 90 days. Access to personal information is restricted to active users and active user accounts only. Access to records containing personal information shall be limited to those persons who are reasonably required to know such information in order to accomplish your legitimate business purpose or to enable us comply with other state or federal regulations.
- Employees and officials are required to report any suspicious or unauthorized use of individuals' personal information immediately to the IT Director.
- Whenever there is an incident that requires notification under M.G.L. c. 93H, §3 (Data Breaches), there will be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible. These post-incident reviews will be conducted by the IT Director and the Town Administrator.
- Employees are prohibited from keeping open files, including electronic files, containing personal information on their desks and desktops while they are away from their work area.
- At the end of the work day, all files and other records containing personal information, including electronic files, must be secured in a manner that is consistent with the WISP's rules for protecting the security of personal information.
- Each department shall develop rules to ensure that reasonable restrictions upon physical access to records containing personal information are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers.
- Access to electronically stored personal information shall be limited to those employees having a unique user-id; and individualized password entry is required when a computer has been inactive for more than ten minutes.

- Unescorted visitors shall not be permitted to visit any area on Town property that contains unsecured personal information.
- Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that complies with M.G.L. c. 93I.
- Violators of the security provisions of this WISP shall be subject to mandatory disciplinary action. (The nature of the disciplinary measures, up to and including termination of employment, will depend on a number of factors, including the nature of the violation and the nature of the personal information affected by the violation.)

VI. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures must be completed on or before June 30, 2016.

External Threats

- The Town shall maintain up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information.
- The Town shall maintain up-to-date versions of system security agent software (anti-virus software) which includes malware protection and up-to-date patches and virus definitions, installed on all systems processing personal information.
- To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted (refer to the Town's Portable Media Policy), as must all records and files transmitted across public networks or wirelessly. Encryption here means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation.
- All computer systems must be monitored for unauthorized use of or access to personal information.
    - There are secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords (3) Control of data security passwords to ensure that such passwords are kept in a secured location and/or format that does not compromise the security of the data they protect (4) restriction of access to active users and active user accounts only and (5) blocking of access to user identification after multiple unsuccessful attempts to gain access.

VII) Questions

If you have any questions or comments about this Policy, please contact the IT Director or the Town Administrator. If you do not have any questions, the Town presumes that you understand and are aware of the rules and guidelines in this WISP and will adhere to them.

VIII. EFFECTIVE DATE OF WISP

The Town of Ayer Written Information Systems Policy (WISP) was approved by the Ayer Board of Selectmen on April 19, 2016 **and was revised and updated on February 20, 2018**

Acknowledgement of Receipt:

I have read, understand and acknowledge receipt of the Town's Written Information Security Policy. I will comply with the guidelines set out in this policy and understand that failure to do so may result in disciplinary action (up to, and including, termination) and/or legal action.

Signed: _____ Date: _____

Printed Name: _____