Town of Southborough

INFORMATION SECURITY POLICY

November 2010

Town of Southborough

Information Security Policy

Introduction

This document represents the Town of Southborough's (Southborough) Information Security Policy (ISP). The ISP was created to formally notify you of the standards the town has established to protect personal information and to provide you with the guidance necessary to comply with these standards.

All municipal employees are subject to the ISP and will receive mandatory, comprehensive training on the policies contained within this document. Should you require clarification regarding any policy, it is your responsibility to contact the Assistant Town Administrator immediately.

During the performance of your official duties, you may have access to various documents, systems or devices containing "personal information." Given the consequences associated with the unauthorized access, loss, theft or disclosure of personal information, the ISP has been implemented to protect Southborough's residents and employees.

Personal Information is defined as an **"individual's first and last name, used with a confidential identifier."** The following is a list of confidential identifiers:

1. **Social security number**
2. **Credit/Debit card number**
3. **Driver's license number**
4. **Financial account number**
5. **Passport number**

The policies contained within this document were created specifically for the Town of Southborough and are therefore not transferable. Any other organization that attempts to reuse the ISP does so at their risk.

Any violation of the policies contained within the ISP may result in disciplinary action, up to and including termination of employment.

Confidentiality and Data Access Policy

1. Any form of personal information that you access must relate directly to your official responsibilities as a Southborough employee.

2. Accessing personal information for training, out of curiosity or for any other non-business reason is strictly prohibited.

3. Personal information must never be left unattended. Any office, file cabinet, desk, workstation, vehicle or storage area containing personal information must be secured when unattended.

4. When you leave your personal or laptop computer unattended, you must "close out" of all applications and reestablish the session upon your return.

5. All forms of personal information must be properly destroyed (shredded) prior to disposal. This requirement applies to any document, computer generated report or other medium on which personal information may be contained.

6. Personal information may never be stored or maintained at any off-site location. This prohibition includes, but is not limited to, a residence, vehicle or commercial storage facility.

7. Employees are strictly prohibited from downloading or installing any software, application or image on their personal computer, or laptop, without the prior, express written authorization of his/her direct supervisor.

8. Personal information may be discussed only with authorized individuals and shared with those who have a specific, municipal business need for such information.

9. Employees are strictly prohibited from remotely accessing any Southborough system, application, database or email account, containing personal information, without the express written permission of his/her direct supervisor.

10. Employees are strictly prohibited from remotely accessing any system, application or database containing personal information, unless he/she utilizes a secure, Virtual Private Network that has been provided by the town.

11. Employees must "close out" of all applications and log-off their personal computer at the conclusion of their work day/night. All computers must be shut off at the conclusion of an employee's tour-of-duty.

12. Any potential loss, theft or misplacement of personal information must be immediately reported to the Assistant Town Administrator.

Password Protection and Acceptable Use Policy

1. Employees are required to protect system passwords from loss, theft and disclosure at all times.

2. "Password sharing", of any type, is prohibited.

3. Employees are strictly prohibited from disclosing their password(s) to anyone. This prohibition includes, but is not limited to, co-workers, supervisors, vendors or family members.

4. Employees are strictly prohibited from maintaining any password, in written form, in an unsecured area. This includes, but is not limited to, maintaining passwords on adhesive notes, under keyboards, beneath desk blotters, under telephones or within any location that may be accessible to another individual.

5. Employees are strictly prohibited from providing their passwords to anyone over the telephone or through email. No individual, organization or government agency is authorized to request your password. Any such inquiry must be immediately reported to your supervisor.

6. Employees are strictly prohibited from maintaining passwords on a cell phone, laptop computer, USB Drive, BlackBerry or similar device.

7. Employees should refrain from reusing passwords that they have used, or are using, for their "personal" accounts. For instance, an employee may not use a "Hotmail" or "AOL" password as their Southborough password.

Email Acceptable Use Policy

1. Opening **non-business** email links, attachments or executable programs is prohibited. This prohibition includes, but is not limited to, email received from family members, personal acquaintances, social networking peers, career sites, advertisers, financial institutions, non-profit and religious organizations,

2. Personal information may only be transmitted within the town's internal email system. Under no circumstances may employees send email, containing personal information, to any external email address unless the message is encrypted.

3. All email encryption technologies, solutions and software must be approved, and provided by, the town.

4. The transmission of personal information using any “Instant Messaging (IM)” method is prohibited. This prohibition applies to all types and variations of this medium.

5. The posting of personal information on social networking sites, peer to peer sites or blogs is prohibited.

6. Employees should exercise extreme caution when receiving email from **unknown,** or **non-business**, sources. Although there may be a legitimate business reason to view an email message from an unknown party, employees are prohibited from clicking on any **link, attachment or executable program** within these messages. (See #1)

Mobile and Portable Storage Device Acceptable Use Policy

1. Employees are prohibited from downloading, transferring, transporting or storing personal information on any laptop computer, external drive, USB drive, compact disc, memory card, magnetic tape, cell phone, BlackBerry, iPhone or other mobile or portable device.

2. Employees are strictly prohibited from installing any software, application or image on any mobile or portable storage device unless previously approved by his/her supervisor.

3. Employees are required to immediately report any loss or theft of a mobile or portable device to the Assistant Town Administrator immediately.

4. Employees are strictly prohibited from maintaining personal information on any unencrypted hard drive (C drive). This prohibition applies to personal computers, laptops, external storage drives and personal digital assistants (PDA).

5. Employees are strictly prohibited from using any personal storage device, such as USB drives, external drives and compact discs, in the workplace.

Incident Response Plan

It is critical that any potential loss, theft, disclosure or other compromise of personal information be reported immediately to your supervisor and the Assistant Town Administrator. It is their responsibility to timely evaluate the nature of the event, document all pertinent information and, if necessary, ensure that the appropriate notifications are made. The following information must be included within the report:

1. Date and time that the event was discovered.

2. Was the loss reported to the police or any third party? If so, obtain copy of the report.

3. Potential witnesses to the event.

4. Location of the event.

5. The specific types of personal information involved.

6. The volume of personal information involved.

7. Whether protective controls were in place.

8. If controls were present, list all measures.

Compliance with All Laws

It is expected that in further compliance with this Information Security Policy, employees will strictly conform with all applicable law, including but not limited to, all public integrity provisions related to the Open Meeting Law, Public Records Law and all State Ethics Standards.

Acknowledgement

I, _____, hereby acknowledge, and represent, that I have read, understand and will adhere to the guidelines contained within the Town of Southborough's Information Security Policy (ISP). I am aware that any violation of the policies contained within the ISP may result in disciplinary action, up to and including termination of my employment.

Signature_____Date_____