Town of Blandford Information Security Policy

It is the policy of the Town of Blandford ("Town") to create and maintain strict controls to protect the personal information of its clients and staff in compliance with MGC Ch. 93H and 93I. To meet this goal, the Town is developing an Information Security Program ("ISP") to institute measures to ensure the integrity, confidentiality, and security of the personal information the Town collects, uses, stores, and disposes. The Town will train every staff member to be aware of and utilize these safeguards. The Town will rely on its managers to exercise due diligence to achieve compliance with the ISP in each Town Department.

Procedure

A. Definitions

1. For the purposes of interpreting this policy, the terms below shall have the following meanings.

   MGL Ch. 93H: known as the "Identity Theft" law, this statute protects Massachusetts citizens in the event their personal information is acquired by an unauthorized person, used for an unauthorized purpose, or information assets are compromised leading to a substantial risk of unauthorized access or use.

   MGL Ch. 93I: known as the "Trash Disposal" law, this statute protects Massachusetts citizens by setting minimum standards for safe and secure disposal of personal information in both paper and electronic form.

   Information Assets: any IT resources, including but not limited to, desk top computers, laptop computers, telephones, fax machines, mobile devices (such as PDA's, flash/thumb drives, Blackberries, cell phones), servers, cables or connecting wires, antennae, video conferencing equipment, video surveillance equipment, tapes, VPN certificates, the Town Portal and website.

   Information Security: measures which protect personal information that the Town collects, uses, stores and disposes.

   Information Security Program ("ISP"): measures the Town has taken or will take in compliance with various laws and other authorities that govern and protect how the Town collects, uses, stores and disposes of personal information.

   Institutional Security Officer ("ISO"): the Board of Selectmen's designee for all issues related to information security; the Board of Selectmen has designated one member of the Board as the ISO.

   Personal Information: information in the Town's possession that readily identifies an individual (typically clients/taxpayers/residents, their families or staff members) and is not otherwise publicly available, including name, identifying

mark or description, social security number, date of birth, driver's license number, state issued identification number, or financial account number.

Reasonable Assurance: achieving the lowest practical level of acceptable risk.

Risks: potential threats to information security or information assets, internal or external, deliberate or accidental, including interruptions to the availability of data, loss of data, breaches of security, unauthorized access to or unauthorized use of personal information.

Security Breach: a break in information security which exposes the Town to any of the Risks listed above.

Unauthorized Person, Access, or Use: an intentional or accidental security breach which results in a person having personal information without authorization, or when a person authorized to access personal information uses it for a purpose outside of the scope of his or her duties.

2. Terms not defined in this policy shall have the meanings assigned to them by reasonably accepted standard dictionary definitions of American English.

B. General Principles

1. All Massachusetts citizens, including Town residents and employees, should be able to expect that government agencies will take reasonable precautions to reduce the risk of identity theft and invasion of privacy through the improper collection, usage, storage and disposal of personal information.

2. To accomplish this goal within Town government, the Town and each of its employees shall undertake measures to protect personal information.

C. The Town's Information Security Program ("ISP")

The Town is creating an ISP to protect personal information and information assets from risks. The Town has taken or will take protective measures, including but not limited to the following:

1. Appoint an ISO;

2. Conduct an assessment of risks to its personal information and assets;

3. Develop internal controls to address identified risks to a level of reasonable assurance;

4. Train employees on the Town's ISP;

5. Perform an annual self-audit to monitor compliance with the ISP;

6. Develop a program to manage and maintain the Town's information assets (such as passwords, logins, encryptions, access reviews, antivirus software, firewalls, data back ups, systems synchronization, data continuity, and disaster recovery);

7. Study ways to ensure that only the minimum quantity of reasonably necessary client and employee information is collected, stored, and used to conduct the Town's business;

8. Design a reporting system for security breaches;

9. Institute measures to permanently dispose of personal information; and

10. Institute any other information protection measures deemed to be reasonably necessary to protect personal information.

D. Responsibilities of All Town Employees

All Town employees shall safeguard the integrity, confidentiality and security of personal information and information assets.

1. Town employees shall use personal information only for authorized purposes.

2. Town employees shall not leave personal information unattended or unsecured (paper or electronic), or use it in conversation where unauthorized persons may overhear the content of the conversation.

3. Town employees shall not share their passwords to any information asset, email or voicemail account and shall not leave a computer without logging off.

4. Town employees sending personal information to printers, fax machines, xerox machines, via email, overnight or regular mail shall make sure to send the information to the right location/recipient.

5. Town employees shall use Town email addresses for conducting Town business. Any/all email regarding official Town business shall be sent from an @townofblandford.com email address. Employees needing access to email should contact the ISO for an email address and login information.

6. Town employees disseminating personal information shall disclose only the minimum quantity reasonably necessary to conduct the Town's business.

7. Town employees shall not save voicemail with personal information unless it is necessary and then only for as long as necessary. When forwarding voicemails, employees shall make sure to send voicemail to the right recipient.

8. Town employees shall not remove personal information from any work location, without the authorization of a supervisor, and shall not store personal information in any non-work location.

9. Town employees shall separate paper trash with personal information and shred it before disposing of it.

10. Town employees shall not copy or share building keys, access codes, electronic credentials, or access cards, or leave windows or doors unsecured in areas where information assets or personal information are located.

11. Town employees shall not install or copy any unauthorized applications onto their workstations without prior written approval from the ISO.

12. Remote access to employee workstations is strictly forbidden and constitutes a serious security threat to the Town. Employees acknowledge this threat and agree that circumventing any safeguards against remote access is strictly forbidden without prior written approval from the ISO.

E. Security Breaches

In the event of a breach or suspected security breach, the employee shall immediately report relevant information to their immediate supervisor. The supervisor shall complete an Information Security Incident Report (see attached and available on the shared drive) and submit it electronically, as soon as practical after discovery of the breach, to the ISO. After reviewing the Report, the Town will make any required notifications, and may deny access to or intentionally disable any of its information assets.

F. Policy Violations

Any Town employee who violates this or any other Town information security policy or procedure may be subject to discipline including termination.

Town of Blandford Information Security Policy Confirmation of Receipt

DATE: _____

This is to certify that I received a copy of the Information Security Policy, whose instructions I have read, and shall observe while in the employ of the Town of Blandford.

_____

(Print) Last Name First Name

Signed _____

Town of Blandford Security Incident Report

Name of reporting individual:
Title of reporting individual:
Town Department/Board/Commission/Agency: Date/Approximate Date of Incident:
Nature of Security Breach (use additional pages if necessary):

Whose personal information was breached, if any (use additional pages if necessary):
What steps have you taken/do you plan to take relating to the incident:

Date:_____

Signature:_____