POLICY # A3-02.1

INFORMATION SECURITY POLICY
ALL EMPLOYEES

Policy

It is the policy of the Town of Wayland ("Town") to create and maintain strict controls to protect the personal information of its employees and those engaged in business with the Town in compliance with M.G.L. c. 93H and 93I. To meet this goal, the Town is establishing 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 rely on its Department Heads to review ISP procedures with its staff and 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.

M.G.L. c. 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.

M.G.L. c. 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 Town Administrator's designee for all issues related to information security; the Town Administrator has designated the Assistant Town Administrator 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/investment/bank 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 the aforementioned 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 following ISP is intended to protect personal information and information assets from risks. The Town may adjust or alter the ISP as it deems necessary:

1. Appoint an ISO;

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

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

4. Have Department Heads review protected personal information within each Department and review with their respective employees their responsibility to ensure that the information is adequately protected;

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

6. Develop a measures to address any identified deficiencies in managing and maintaining 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. Collect, store and use only the minimum quantity of reasonably necessary protected information in conducting Town business;

8. Establish a reporting mechanism 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 acquire and use personal information only for authorized Town purposes.

2. Town employees shall not knowingly 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 approved passwords for any information asset, email or voicemail account with anyone who is not also approved for access to protected information.

4. Town employees shall not leave personal computers with access to programs containing protected information unattended and at risk for unauthorized access.

5. Town employees sending personal information to printers, fax machines, copying machines, via email, overnight or regular mail shall make every effort to ensure the information is sent to the right location/recipient and only to that location/recipient.

6. Town employees disseminating personal information shall disclose only the minimum information 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 every effort to send voicemail to the right recipient.

8. Town employees may remove personal information from the information's customary work location only if such removal is necessary and only if such removal has been authorized in writing by a supervisor, which authorization shall specify the duration and location of removal. In the case of laptops and/or computer discs or data storage devices which contain personal information and the removal of which is authorized in accordance with the preceding sentence, such laptops, computer discs or data storage devices shall be kept by the employee in their presence or in a secure location at all times during the authorized removal. Town employees shall not store personal information in any non-work location.

9. Town employees shall make every effort to separate paper trash and recycled paper with personal information from other trash and recycled paper and shall shred it before disposing of it.

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

11. If necessary, employees will be provided training pertinent to the provisions of this policy.

E. Security Breaches

In the event of a security breach or suspected security breach, the employee shall immediately report relevant information to their Department Head. The Department Head shall notify the ISO as soon as possible after the discovery of the breach and shall provide a written report of the breach or suspected breach to the ISO. After reviewing the report, the Town will make any required notifications, and may restrict access to or intentionally disable any of its information assets.

F. Policy Violations

Any Town employee who recklessly or intentionally violates this or any other Town information security policy or procedure may be subject to disciplinary action up to and including termination from employment.

Town Administrator Revised: January 10, 2011

Information Security Policy – Department Receipt & Review

DATE: _____

This is to certify that I have met with the employees in the _____ Department regarding the security of protected information. Copies of the Information Security Policy were distributed to all employees (signed acknowledgement attached).

_____

(Print) Last Name First Name

Signed _____

Department Head

Information Security Policy – Employees' Receipts of Policy

_____ Department

Print Name	Signature	Date
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____