FIRST UNITARIAN SOCIETY IN NEWTON

FUSN Issuance 2010-05 ☑ **Policy** ☐ **Information**

From: Pat Rohan
Chair, Operations Council

Date: April 20, 2010

Subject: **Written Information Security Plan ("WISP")**

Purpose: To establish a WISP to enable compliance with the Massachusetts Privacy Law (201 CMR 17.00) for the Protection of Personal Information.

Background: The Commonwealth of Massachusetts enacted The Massachusetts Privacy Law 201 CMR 17.00. This law was enacted in the wake of security breaches at high profile companies doing business in Massachusetts and mandates new steps to protect information falling within the scope of the law.

The scope of the law extends to any organization (other than certain government entities) which "receives, maintains, processes or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Under the law, "Personal Information" is defined as:

- a Massachusetts resident's name combined with a complete social security number, driver's license, or other state-issued number
- a Massachusetts resident's name combined with a financial account number or a complete credit card or bank account number.

The scope of the law does not extend to any information that is lawfully obtained from publicly available sources or from federal, state or local government records that lawfully are made available to the general public. Use of the term Personal Information hereinafter

in this Policy is meant to refer only to that falling within the definition of 201CMR 17.00.

The deadline for full compliance with 201CMR 17.00 is March 1, 2010 and compliance consists principally of having an approved WISP in place by that time.

Current Situation:

The FUSN Administrator in consultation with the Treasurer has made an assessment and inventory of Personal Information falling within the scope of 201CMR 17.00 at FUSN. This Personal Information, which consists of social security numbers maintained in IRS and related payroll documents and photocopies of certain checks made out to FUSN, is secured in locked filing cabinets in the FUSN office.

Personal Information of the FUSN staff is stored electronically on only FUSN's computers which do not access the internet or email and this information also is provided to FUSN's third party payroll service provider, ADP. FUSN also has a third party contract bookkeeper who is engaged annually by FUSN in a written contract which includes a confidentiality clause. The external bookkeeper has occasional access to the FUSN office and computers but does not store Personal Information of FUSN staff, members or friends.

Personal Information is not and will not be received, maintained, processed or accessed through the FUSN website: www.fusn.org.

Access to Personal Information at present is limited to the FUSN Administrator, Treasurer and Assistant Treasurers (2). The policies described below are intended to establish a WISP that takes into account the amount, use, nature and quantity of Personal Information falling within the scope of the Massachusetts Privacy Law.

Policy: FUSN WISP is attached below

Effective Date: March 1, 2010

FUSN Written Information Security Plan "WISP"

1. The FUSN Administrator is appointed as FUSN's information security coordinator acting in consultation with the Operations Council. As such the Administrator will be responsible for implementation and ongoing compliance with FUSN's WISP as well as advising the Operations Council of any physical or electronic threats to the security of Personal Information at FUSN that should be addressed through revisions to this WISP.

2. Personal Information falling within the scope of the Massachusetts Privacy Law at FUSN is as defined above in "Personal Information at FUSN." No other information falling within the scope of the Massachusetts Privacy Law will be received, maintained, processed or accessed by anyone without the express permission of the Administrator and without fully complying with this Policy.

3. This policy will be published on the FUSN web site and given to all FUSN staff, members of the Operations Council and Board of Trustees. The Administrator should document receipt of this policy for each staff member.

4. Written records containing Personal Information shall, at all times, be locked (in a separate file cabinet) in the FUSN office when not being used. The office will be locked when the Administrator or the Treasurer or an Assistant Treasurer is not physically present in the office. It is anticipated that only the Administrator and Treasurer have an ongoing need for access to this Personal Information and access by others will be on an exception basis with the concurrence of the Administrator and Treasurer.

5. Keys to the locks securing the Personal Information shall be held by the Administrator and Treasurer only.

6. Personal Information shall be stored only on FUSN computers that are not used to access the internet or email networks. This part of policy is explicitly to avoid the need for encryption of data and any change to this part would require a review of the need for the implementation of encryption software.

7. Access to FUSN computers containing Personal Information shall be given only by the Administrator and limited to the Administrator, Treasurer, Assistant Treasurers and third party bookkeeper protected by user IDs and passwords.

8. Passwords shall, at a minimum contain one upper case letter, one lower case letter, one numerical character and one non numerical character. Passwords shall be changed at least every ninety days and upon the termination of employment of any FUSN staff member having had access to FUSN's computers.

9. The Administrator shall obtain confirmation from every third party service provider to FUSN of their compliance with 201 CMR 17.00 if they receive, access, process,

or maintain Personal Information as part of their services to FUSN.

10. Written records containing Personal Information will be retained for a period not longer than required by law or applicable regulations and shredded prior to disposal.

11. Compliance with this plan shall be reviewed at least annually by the FUSN Operations Council with the Administrator or whenever deemed necessary by the Operations Council due to a material change in business practices or other reason.

12. The Administrator or any person who becomes aware of a violation of this policy or unauthorized access to Personal Information shall immediately inform the Chair of the Operations Council who shall take whatever action is deemed appropriate in consultation with the Senior Minister, Board of Trustees and Steering Committee if necessary.