Comprehensive
Written Information Security Program

for the

First Congregational Church
of Georgetown, UCC

Comprehensive Written Information Security Program for Compliance with 201 CMR 17.00

Appendix

Comprehensive Written Information Security Program

for Compliance with 201 CMR 17.00

201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth is the regulation that implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information (PI) about a resident of the Commonwealth of Massachusetts. As a part of the requirements of this regulation, the First Congregational Church of Georgetown, UCC is creating, implementing and training employees on this Written Information Security Program (WISP*)*

1. Objective and Scope

This comprehensive Written Information Security Program (WISP*)* has been developed to ensure that the First Congregational Church of Georgetown, UCC has the procedures in place to protect the personal information (PI) of our guests, members, and employees in compliance with 201 CMR 17.00. The WISP evaluates any foreseeable risks and the steps that will be taken to minimize those risks.

For purposes of this WISP, "personal information" means a Massachusetts 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 that resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit/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.

The WISP will be reviewed regularly, and the effectiveness of all safeguards will be continually monitored.

2. Data Security Manager

The First Congregational Church of Georgetown, UCC will designate, on an annual basis, the nominated Finance Team Chair (considered the Treasurer of the corporation) as **Data Security Manager** to oversee the protection of all PI. The Finance Team Chair, along with the elected bookkeeper and the Church's settled pastor, will be the sole holders of personal information pertaining to all employees, including I9s, W4s and W2s, and volunteers of the church, including Vehicle Operator Information Forms.

The Finance Chair and the bookkeeper will maintain all of the electronic tax records for employees, and they will:

a. ensure that all data entry of PI be performed in a secure manner, never transferring PI by email for any reason, and at no time taking any written form of PI off the Church premises;

b. ensure that all electronic data storage will be in secure password protected format;

c. provide appropriate data security protection, including firewalls and virus scanning software reasonably designed to maintain the integrity of PI, on any personal computer used when performing the jobs of Finance Team Chair and bookkeeper, ensuring that updates are performed on a regular basis;

d. keep any personal computer used in conjunction with the jobs of Finance Team Chair and bookkeeper physically secure whenever traveling with said computer

e. ensure that any transfer of data for tax purposes will be done only on government approved websites.

f. ensure that any paperwork containing personal information is shredded as soon as it is no longer required to be retained.

The pastor will ensure that paper records containing personal information which are required to be retained as part of an employee's file, including records for any terminated employee, are kept in a locked file cabinet in the pastor's office. The pastor's office will be locked whenever the pastor is not present for any length of time. Keys to the locked cabinet are held by the pastor; keys to the pastor's office are held by the pastor and the office manager.

Any unauthorized use or access to records containing PI will be immediately assessed to determine the extent of the breach of security. The appropriate authority will be advised when necessary, and updates will be made to the specified safeguards in this WISP to prevent future unauthorized use/access.

3. Data Security Coordinator

The First Congregational Church of Georgetown, UCC will designate, on an annual basis, one member of the Finance Team as **Data Security Coordinator** for the church. This individual will:

a. initiate updates to the WISP at least annually;

b. advise all church employees and volunteers who handle PI of any kind on the requirements of the WISP and on the importance of maintaining the security measures set forth in this document;

c. review the procedures outlined in the WISP whenever there is a change in business practices that may impact the security or integrity of records containing personal information and making changes when necessary;

d. ensure that any third-party provider contract or agreement includes language that states they are in compliance with 201 CMR 17.00;

e. assess the extent of any known breach of security and notifying the appropriate authority if it is deemed necessary;

f. ensure that any records of a known breach of security be stored in the same manner as all other PI detailed herein, and that a post-incident review is conducted with the Data Security Manager;

g. review saved paperwork on an annual basis, utilizing legal requirements and government timeframes, then shredding items no longer needed.

4. Risks and Safeguards

The First Congregational Church of Georgetown, UCC does not keep any personal financial information pertaining to any guest, member or employee for any reason. All checks received for pledges, contributions/donations, usage of the facility, and fundraisers are taken to the bank and deposited as soon as possible. The church does not accept credit card payments.

Some of the church's members pay their pledged amounts through Vanco Services, a third-party provider designated for processing electronic funds transfers. Church members are required to sign up for this service personally, and their account information is not held by the church. Vanco Services is required to provide the church with a written contract or agreement that states they are in compliance with 201 CMR 17.00.

The church may, at times, consult an outside auditor to review and assess all of the records of the church. Any auditor hired to perform such tasks will be required to provide the First Congregational Church of Georgetown, UCC with a written contract or agreement that states they are in compliance with 201 CMR 17.00. Any electronic transfer of data between the Finance Team Chair, the bookkeeper, and an auditor will be conducted only through a secure, encrypted website and only when deemed necessary by the Finance Team of the church to complete the audit process.

.

Appendix

Requirements for Security Breach Notifications under Chapter 93H

Pursuant to M.G.L.c.93H, s.3(b), if you own or license data that includes personal information of a Massachusetts resident, you are required to provide written notice as soon as is practical and without unreasonable delay to:

1. The Attorney General (AGO);

2. The Director of the Office of Consumer Affairs and Business Regulation (OCABR); and

3. The affected Massachusetts resident

when you know or have reason to know (a) of a breach of security; or (b) that personal information of a Massachusetts resident was acquired by or used by an unauthorized person or for an unauthorized purpose.

Notice to the AGO and OCABR

The notice to the Attorney General and the Director of Consumer Affairs and Business Regulation shall include, but not be limited to: (1) the nature of the breach of security or the unauthorized acquisition or use; (2) the number of Massachusetts residents affected by such incident at the time of notification; and (3) any steps the person or agency has taken or plans to take relating to the incident.

To assist you in this notification process, the AGO has prepared a sample letter outlining the minimum information that your notice should contain to the Attorney General. To download and view:

Notice to Affected Massachusetts Residents

A person or agency that has experienced a breach of security or the unauthorized acquisition or use of personal information of Massachusetts residents must also provide notice to those affected Massachusetts residents. This notice shall include, but not be limited to:

1. the consumer's right to obtain a police report;

2. how a consumer requests a security freeze;

3. the necessary information to be provided when requesting the security freeze; and

4. any fees to be paid to any of the consumer reporting agencies, provided however, that the notification shall **not** include the nature of the breach or unauthorized acquisition or use; or the number of Massachusetts residents affected by the security breach or the unauthorized access or use.

To assist you in this notification process, we have prepared a sample letter outlining the minimum information that your notice should contain to the affected Massachusetts resident(s). To download and view:

SAMPLE LETTER TO ATTORNEY GENERAL

Date

Attorney General Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

Dear Attorney General Coakley:

Pursuant to M.G.L. c. 93H, we are writing to notify you of [a breach of security/an unauthorized access or use of personal information] involving [number] Massachusetts resident[s].

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS
[This paragraph should provide the date of the incident, a summary of the nature of the incident, a description of the categories of personal information involved in the incident, and whether the personal information that was the subject of the incident was in electronic or paper form].

NUMBER OF MASSACHUSETTS RESIDENTS AFFECTED
[This paragraph should specify the number of affected individuals residing in Massachusetts whose personal information was the subject of the incident. This paragraph should also indicate that these Massachusetts residents have received or will shortly receive notice pursuant to M.G.L. c. 93H, s. 3(b) and should specify the manner in which Massachusetts residents have or will receive such notice. You should also include a copy of the notice to affected Massachusetts residents in your notification to the Attorney General].

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT
[This paragraph should outline all the steps you have taken or plan to take relating to the incident including, without limitation, what you did when you discovered the incident; whether you have reported the incident to law enforcement; whether you have any evidence that the personal information has been used for fraudulent purposes; whether you intend to offer credit morning services to consumers; and what measures you have taken to ensure that similar incidents do not occur in the future.]

OTHER NOTIFICATION AND CONTACT INFORMATION
[Finally, your letter should indicate whether you have provided similar notification to the Director of Consumer Affairs and Business Regulation. You should also include the name and contact information for the person whom the Office of the Attorney General may contact if we have any questions or need further information.]

SAMPLE LETTER TO AFFECTED MASSACHUSETTS RESIDENTS

Date

Consumer Name
Address
City, MA

Dear _____:

We are writing to notify you that a [breach of security/unauthorized acquisition or use] of your personal information occurred on [date(s)].

YOUR NOTICE MUST INCLUDE THE FOLLOWING INFORMATION:

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

[**NOTE: Although not required by M.G.L. c. 93H, you should also consider providing the affected Massachusetts residents with additional information to protect themselves against identity theft or other fraud including, but not limited to: the placement of fraud alerts on their credit file; the need to review their credit reports for unexplained activity; and the need to review credit card or other financial accounts for any suspicious and/or unauthorized activity. Many companies provide affected Massachusetts residents with free credit monitoring services. If you are providing credit monitoring services for affected Massachusetts residents, you should provide them with information concerning how they may enroll for such credit monitoring services as well as any telephone numbers or websites that you have set up to answer any questions they may have concerning the incident. Please note that any additional advice provided to affected Massachusetts residents may vary on a case-by-case basis and these information suggestions are not a complete list of all the information that you may want to provide affected Massachusetts residents to better protect themselves against identity theft or fraud].**

If you should have any further questions, please contact [provide contact information].

Sincerely,