

# **Faith Community Church**

## **Written Information Security Policy**

### **I. OBJECTIVE:**

The Faith Community Church's objective, in the development and implementation of this Written Information Security Plan ("Plan"), is to create effective administrative, technical and physical safeguards for the protection of 'personal information' of residents of the Commonwealth of Massachusetts, and to comply with the Church's obligations under 201 CMR 17.00. The Plan sets forth the Church's procedure for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting, maintaining, and protecting 'personal information' of residents of the Commonwealth of Massachusetts. For purposes of this Plan, '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 such resident: (a) social security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or 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.

### **II. PURPOSE:**

The purpose of the Plan is to:

- a. Ensure the security and confidentiality of 'personal information';
- b. Protect against any anticipated threats or hazards to the security or integrity of such information; and
- c. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

### **III. SCOPE:**

In formulating and implementing the Plan, the Church will (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing 'personal information'; (2) assess the likelihood and potential damage that could result from these threats, taking into consideration the sensitivity of the 'personal information'; (3) evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks; (4) design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and (5) regularly monitor the effectiveness of those safeguards.

#### **IV. DATA SECURITY COORDINATOR:**

The church has designated Linda Grant as the Data Security Coordinator (“DSC”) to implement, supervise and maintain the Plan. The DSC shall report to the Executive Director of the Church with respect to the Plan. The DSC shall be responsible for:

- a. Initial implementation of the Plan;
- b. Training employees;
- c. Regular testing of the Plan's safeguards;
- d. Evaluating the ability of each of the Church’s third-party service providers to protect, in the manner required by 201 CMR 17.00, the ‘personal information’ to which the Church has permitted them access; and taking the steps reasonably necessary to ensure that such third-party service providers are applying to such ‘personal information’, protective security measures at least as stringent as those required to be applied under 201 CMR 17.00;
- e. Reviewing the scope of the security measures in the Plan at least annually, or whenever there is a material change in business practices that may implicate the security or integrity of records containing ‘personal information’;
- f. Will ensure employees read the WISP policy and implementation plan and turn in a signed statement documenting they have done so. This will be done annually.
- g. Coordinating with other Church personnel to assist with implementation of the Plan, including personnel to assist with Information Technology issues, Human Resources issues, facilities maintenance and support, and legal compliance.

#### **V. INTERNAL RISKS:**

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing ‘personal information’, and to evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, the below-listed measures are mandatory and are effective immediately. To the extent that any of these measures require a phase-in period, such phase-in must be completed on or before March 1, 2010. Oversight for implementation of these measures is the responsibility of the DSC.

- a. A copy of the Plan must be distributed to each employee who shall, upon receipt of the Plan, acknowledge in writing that he/she has received a copy of the Plan. New employees are to receive a copy of the Plan during orientation.
- b. Because Faith Community Church is considered a low risk threat, employees will be required read the WISP policy and implementation plan and turn in a signed statement documenting they have done so. This will be done annually. In addition, new employees will be required to follow the same requirement. Copies of signed statements will be kept in the employee’s personal folder.

- c. Employment contracts must be reviewed and amended, as necessary, to require compliance with the provisions of the Plan, and to prohibit any nonconforming use of 'personal information' during or after employment.
- d. The amount of 'personal information' collected must be limited to that amount reasonably necessary to accomplish legitimate business purposes, or as necessary to comply with other state or federal regulations. The DSC is responsible for compiling and maintaining a "Personal Information Record Location List, which sets forth the locations and description of all records containing 'personal information' in either hard copy or electronic form. Such list shall also include a listing of third-party vendors or service providers that have been provided with 'personal information'.
- e. Access to records containing 'personal information' shall be limited to only those employees who are reasonably required to have access in order to accomplish their job duties and responsibilities, or as is otherwise necessary to comply with state or federal regulations. Except as expressly authorized in writing by the DSC, employees are prohibited from keeping, accessing and/or transporting 'personal information' off the Church's premises.
- f. When applicable electronic access to systems containing 'personal information' will be blocked following multiple unsuccessful attempts to gain access due to improper user identification or password.
- g. All security measures shall be reviewed at least annually by the DSC and his/her designees, or whenever there is a material change in church practices that may reasonably implicate the security or integrity of records containing 'personal information'. The DSC shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.
- h. Terminated employees must return all records containing 'personal information', in any form, that may at the time of such termination be in the former employee's possession, custody or control (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).
- i. A terminated employee's physical and electronic access to 'personal information' must be blocked immediately prior to the employment termination or during the termination meeting. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the Church's information. Moreover, simultaneously, such terminated employee's remote electronic access to 'personal information' must be disabled; and his/her voicemail access, e-mail access, internet access, and passwords must be invalidated. The DSC shall maintain a secured master list of all lock combinations, passwords and keys.

- j. Current employees' user-IDs and passwords must be changed annually as directed by the DSC.
- k. Access to 'personal information' shall be restricted to active users and active user accounts only. 'Personal information' access is restricted to those employee who have a "need to know" to perform the job. Files accessed by "need to know" employees will be password protected.
- l. Employees are required to report any suspicious or unauthorized access to, or use of, 'personal information'.
- m. Whenever there is an incident involving 'personal information' that requires notification under M.G.L. c. 93H, §3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in the Church's security practices are required to improve the security of 'personal information' for which the Church is responsible. In documenting an incident involving a breach of security measures related to protection of 'personal information', the DSC will generate an incident report that addresses, at a minimum: (i) review of the security breach; (ii) the responsive actions taken in connection with the breach; and (iii) those revisions to the Plan or the Church's business practices that were made to minimize the likelihood of a reoccurrence of the same, or a similar, breach. Notification of a breach, if required pursuant to M.G.L. c. 93H, shall be handled by the Church's General Counsel, in consultation with the DSC and Church management.
- n. Employees are prohibited from keeping open files containing 'personal information' on their desks when they are not at their desks.
- o. At the end of the work day, all files and other records containing 'personal information' must be secured in a manner that is consistent with the Plan's rules for protecting the security of 'personal information', including ensuring that hard copies of 'personal information' are placed in a secure, locked file or area.
- p. Access to electronically-stored 'personal information' shall be electronically limited to those employees having a unique log-in ID, and re-login shall be required when a computer has been inactive for more than 15 minutes.
- q. Visitors' access to areas in which 'personal information' is stored must be restricted. Visitors shall not be permitted to visit unescorted any area within the Church Office premises that contains 'personal information'. Church staff members are authorized to challenge anyone who is unknown to them or acting in a suspicious manner. The DSC is responsible for reviewing and approving measures related to visitor access and for identifying all areas containing 'personal information' prior to March 1, 2010.
- r. Paper or electronic records (including records stored on hard drives or other electronic media) containing 'personal information' shall be disposed of only in a

manner that complies with M.G.L. c. 93I. For example, all physical copies (and originals) of records containing ‘personal information’ that are designated for destruction shall be shredded so that no ‘personal information’ contained on them can be practicably read or reconstructed. All electronic versions of records containing ‘personal information’ shall be destroyed or erased so that no ‘personal information’ contained on them can be practicably read or reconstructed.

- s. The DSC and/or his/her designee shall review prior to March 1, 2010, all third-party service provider relationships and contracts to (i) verify that the third-party service providers have the capacity to protect ‘personal information’ in compliance with 201 CMR 17.00; (ii) confirm that the third-party service providers are applying protective security measures that are at least as stringent as those required under 201 CMR 17.00; and (iii) ensure that contracts are amended to provide a representation by the third-party service provider that it has implemented a written information security program in compliance with 201 CMR 17.00 and that such program applies protective security measures at least as stringent as those required under 201 CMR 17.00.
- t. The DSC and/or his/her designee shall review all new agreements with third-party service providers to ensure compliance with this Plan. In addition, the DSC shall conduct an annual review of third-party service provider agreements to ensure continuing compliance. To facilitate monitoring/review efforts, the DSC shall maintain an updated listing of all existing third-party service providers and their respective contracts.
- u. The DSC will have authority, in consultation with church management, to impose disciplinary measures, up to and including termination of employment, to any employee who violates the policies and procedures set out in this Plan.

## **VI. EXTERNAL RISKS:**

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing ‘personal information’, and to evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, the below-listed measures are mandatory and are effective immediately. To the extent that any of these measures require a phase-in period, such phase-in must be completed on or before March 1, 2010. Oversight for implementation is the responsibility of the DSC.

- a. There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the ‘personal information’, installed on all systems processing ‘personal information’.
- b. There must be reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems that process ‘personal information’.
- c. It is the policy of Faith Community Church that ‘personal information’ will NOT be stored or transported on laptops or other portable devices.

- d. All computer systems must be monitored for unauthorized use of, or access to, 'personal information'.
- e. There must be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (4) restriction of access to active users and active user accounts only; and (5) blocking of access to user identification after multiple unsuccessful attempts to gain access.
- f. The secure access control measures in place must include assigning unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access to 'personal information'.
- g. Establish systems and procedures for secure back-up, storage and retrieval for computerized records containing 'personal information'.
- h. Establish procedures to ensure external points of entry to the office are closed, locked and inaccessible to unauthorized persons when the office is closed.
- i. Install alarm or other security systems, with training for authorized persons on activation and deactivation.
- j. Physically lock or otherwise secure the computer room, and if necessary, all areas in which paper records are maintained.

## **VII. ADDITIONAL EMPLOYEE OBLIGATIONS:**

In addition to the other responsibilities set out in this Plan, all employees shall be responsible for:

- a. Regularly reviewing the Plan, including all revisions and updates that are made to the Plan;
- b. Complying with all policies and procedures that have been developed and implemented as a result of the Plan;
- c. Reviewing all internal and external risks identified in the Plan in order to be more aware of potential threats to the integrity and security of 'personal information';
- d. Providing feedback and suggestions to the DSC relating to the Plan;
- e. Reporting to the DSC all suspicious activity relating to 'personal information', including without limitation, unauthorized access to, or use of, 'personal information' by other employees, or

- f. Immediate reporting of any security breach to the DSC;
- g. Protecting assigned passwords so that they are not accessible or used by any other party; and
- h. Complying with all requirements for the return and safeguarding of 'personal information' upon employment termination.

WISP Implementation Plan may be obtained from the Data Security Coordinator.

**Written Information Security Policy and Implementation Plan**

**Signature Page**

I have read and understand the Written Information Security Policy and Implementation Plan as it applies to the Faith Community Church.

Please print this page. Sign and print your name and date this form. Return the completed signature page to the Data Security Coordinator. (Note: this page will be filed in your personnel folder.)

Thank you.

\_\_\_\_\_  
Name (print)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature