Roman Catholic Archdiocese of Boston 401(k)
Retirement Savings Plan
Roman Catholic Archdiocese of Boston Pension Plan
Roman Catholic Archdiocese of Boston Health Benefit Trust
Roman Catholic Archdiocese of Boston Life and LTD Trust Roman Catholic Archdiocese of Boston Transition Assistance Program
(collectively, the "Benefit Trusts")

ELECTRONIC DATA SECURITY POLICY

I. OBJECTIVE:

It is the objective of the Benefit Trusts, in the development and implementation of this comprehensive written information security program ("WISP"), 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 obligations under 201 CMR 17.00. This WISP sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of The Commonwealth of Massachusetts. This policy applies to all employees, contractors, temporary workers or other staff members of the Benefits Office of the Archdiocese.

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 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 this WISP is to:

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

III. SCOPE:

In designing and implementing this WISP, we have, (1) identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (2) assessed the likelihood and potential damage of these threats, taking into consideration the amount and sensitivity of the personal information; and (3) evaluated the sufficiency of existing policies, procedures, and other safeguards in place to control risks, including training, employee compliance, and means of detecting system failures. We will regularly monitor the effectiveness of these safeguards. We will re-evaluate each of these elements as needed.

IV. DATA SECURITY COORDINATOR:

The Benefit Trusts have designated Plan Administrator Carol Gustavson to implement, supervise and maintain this WISP. That designated employee (the "Data Security Coordinator") will be responsible for:

a. Initial implementation of this WISP;

b. Training employees;

c. Regular monitoring and testing of this WISP's safeguards, and recommending and implementing improvements as necessary;

d. Evaluating the ability of each of our third-party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, consistent with 201 CMR 17.00; and requiring such third party service providers by contract to implement and maintain appropriate security measures with respect to personal information.

e. Reviewing the scope of the security measures in this WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information.

f. Conducting an annual training session on the elements of this WISP for all employees, volunteers, and independent contractors, including temporary and contract employees who have access to personal information.

g. Documenting responsive actions taken in connection with any incident involving a breach of security.

h. Conducting a post-incident review and documenting actions taken in response to the incident to ensure personal information security.

i. In case of a security breach or the loss of control of any personal information, contacting the Archdiocese Office of General Counsel and/or legal counsel for the Trusts for guidance on proper reporting procedures.

V. INTERNAL RISKS:

In order to combat internal risks to the security, confidentiality, and integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures will be taken:

A copy of this WISP must be distributed to each employee of the Archdiocese Benefits Office.

Employees will be trained on the detailed provisions of this WISP.

Disciplinary action will be taken for violation of security provisions of this WISP.

Access to electronic records containing personal information will be limited to those persons who are reasonably required to have access to such information to perform their job duties. Access to physical records will be reasonably limited.

Electronic access to systems under a user identification will be blocked after multiple unsuccessful attempts to gain access.

All security measures will be reviewed at least annually and whenever there is a material change in our practices that may reasonably implicate the security or integrity of records containing personal information. Appropriate upgrades to the security system will be implemented as needed.

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 (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

A terminated employee's physical and electronic access to personal information must be immediately blocked. Such terminated employee must surrender all keys, IDs, or access codes or badges, business cards, and the like, that permit access to the premises or personal information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated. The Data Security Coordinator shall maintain a highly secured master list of all lock combinations, passwords and keys.

Current employees' user IDs and passwords must be changed periodically.

Access to personal information will be restricted to active users and active user accounts only.

Employees are encouraged to report any suspicious or unauthorized use of personal information.

Whenever there is a breach of security, 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 our security practices are required to improve the security of personal information for which we are responsible.

Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.

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 this WISP's rules for protecting the security of personal information.

We will develop rules that ensure that reasonable restrictions upon physical access to records containing personal information are in place, and we will store such records and data in locked facilities, secure storage areas or locked containers.

Transport of files containing personal information outside the premises will not be permitted except in cases of need and only with the use of reasonable precautions to ensure the security of the personal information.

Access to electronically stored personal information will be electronically limited to those employees having a unique log-in ID and password that is not a vendor-supplied default; and re-log-in shall be required when a computer has been inactive for more than a fifteen minutes.

Visitors' access must be restricted to one entry point for each building in which personal information is stored. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.

When disposing of records containing personal information, we will redact, burn, pulverize or cross-shred paper documents so that personal data cannot practicably be read or reconstructed. When disposing of electronic records containing personal information, we will destroy or erase such records so that personal information cannot practicably be read or reconstructed.

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 evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures will be taken:

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.

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 processing personal information.

To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly.

All computer systems must be monitored for unauthorized use of or access to personal information.

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 or format that does not compromise the data's security.