_____, INC.

WRITTEN INFORMATION SECURITY PROGRAM (WISP)
FOR PROTECTION
OF PERSONAL INFORMATION

I. GENERAL

A. Objective of WISP

The objective of _____, Inc. (the "Corporation"), in the development and implementation of this comprehensive Written Information Security Program ("WISP"), 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 Corporation's obligations under M.G.L. c. 93H, M.G.L. c. 93I, and 201 CMR 17.00.

The WISP sets forth the Corporation's procedure for evaluating the Corporation's electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Personal Information of residents of the Commonwealth of Massachusetts.

For purposes of this WISP, "Personal Information " means the following, whether in paper, electronic or other form:

1. a Massachusetts resident's first name and last name or first initial and last name;
2. 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).

"Board Member" shall mean a Corporation board of directors member with access to Personal Information.

B. Purpose of WISP

The purpose of the Corporation's WISP is to:

1. ensure the security and confidentiality of Personal Information;

2. protect against threats or hazards to the security or integrity of such information; and
3. protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

C. Scope of WISP

In formulating and implementing the Corporation's WISP, the intended scope is to do the following:

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 of 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 WISP 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.

D. Data Security Coordinator:

The Corporation has designated the Executive Director to be the Corporation's Data Security Coordinator. He or she will be responsible for implementing, supervising and maintaining the Corporation's WISP, including:

1. initial implementation of the Corporation's WISP;
2. training of the following persons regarding the Corporation's WISP and Personal Information security: (a) all employees; (b) Board Members (see Part I.A on page one for definition of "Board Member");
   (c) independent contractors with access to Personal Information; and
   (d) any other person involved with the Corporation who has or will have access to Personal Information;
3. regular testing of the WISP's safeguards;
4. evaluating the ability of each of the Corporation's third party service providers to implement and maintain appropriate Personal Information security measures for the Personal Information to which the Corporation has permitted them access, consistent with 201 CMR 17.00, and requiring such third party service providers by contract to implement and maintain appropriate Personal Information security measures;
5. Reviewing the scope of the Personal Information security measures in the 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.

E. Limits on Collection and Storage of Personal Information at the Corporation

1. The Corporation is in possession of Personal Information of Massachusetts residents both as an employer and as a nonprofit organization.
2. As an employer, the Corporation possesses Personal Information for its employees. The Personal Information that is collected and stored from each employee shall be limited to: that information which is necessary for employment, such as tax forms; that information which is voluntarily provided to obtain certain benefits of employment, such as pension, health, life and disability insurances; and that information which is necessary for the Corporation to comply with state or federal laws and regulations.
3. As part of its legitimate organizational purpose, the Corporation possesses Personal Information of Massachusetts residents obtained during the course of the Corporation's activities. The Personal Information that is collected and stored shall be limited to: that information which is reasonably necessary to accomplish the Corporation's legitimate organizational purpose; and that information which is necessary for the Corporation to comply with state or federal laws and regulations.

F. Review of WISP and Procedures

The Corporation's WISP and all security measures and procedures shall be reviewed at least annually and, in addition, whenever there is a material change in the Corporation's business practices that may reasonably implicate the security or integrity of records containing Personal Information. The Data Security Coordinator shall be responsible for this review and shall fully apprise the Organization's Board of the results of that review and any recommendations for improved security arising out of that review.

II. PROTECTIONS AGAINST INTERNAL DATA SECURITY BREACH

To combat internal 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 are mandatory and are effective immediately:

A. Information and Access

1. The amount of Personal Information collected shall be limited to that amount reasonably necessary to accomplish the Corporation's legitimate business purposes, or necessary to the Corporation to comply with other state or federal regulations.
2. Access to records containing Personal Information shall be limited to those persons who are reasonably required to know such information in order to accomplish the Corporation's legitimate business purpose or to enable the Corporation to comply with other state or federal regulations.
3. Access to electronic Personal Information shall be restricted to active users and active user accounts only.
4. Access to electronically stored Personal Information shall be electronically limited to those employees or Board Members (see Part I.A on page one for definition of "Board Member") having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes.
5. Paper or electronic records (including records stored on hard drives or other electronic media) containing Personal Information shall be disposed of only in the following manner, in compliance with M.G.L. c. 93I:
    a. paper documents containing Personal Information shall be either redacted, burned, pulverized or shredded so that Personal Information cannot practicably be read or reconstructed; and
    b. electronic media or other non-paper media containing Personal Information shall be destroyed or erased so that Personal Information cannot practicably be read or reconstructed.

B. Board Members and Employees

1. A copy of the WISP must be distributed to each employee, including part-time, temporary and contract employees, and to each Board Member (see Part I.A on page one for definition of "Board Member"). As a condition of their employment or Board service, all employees and Board Members must sign an acknowledgement and certification (see Acknowledgement & Certification at the end of this document) that they have received a copy of the Corporation's WISP and that they will comply with the provisions of the WISP. These signed acknowledgements and certifications shall be retained by the Data Security Coordinator.
2. There must be regular training of employees and Board Members on the detailed provisions of the WISP, including training at the inception of a new employee's employment or new Board Member's board service. The Data Security Coordinator shall organize such training.

3. Employees and Board Members are prohibited from keeping unsecured files containing Personal Information in their work area when they are not present, or otherwise failing to take reasonable measures to protect the security of Personal Information.
4. At the end of the work day, all files and other records containing Personal Information must be secured in a manner that protects the security of Personal Information.
5. All employees and Board Members are required to comply with the provisions of the WISP, and if the security provisions of the WISP are violated by an employee, the Data Security Coordinator or, in the case of a Board Member, the Corporation's board of directors shall implement the following disciplinary procedure:
    a. For minor infractions, with the definition of "minor" to be determined by the Data Security Coordinator or the board of directors based upon the nature of the violation and the nature of the Personal Information affected by the violation, the employee or Board Member shall be disciplined by either a verbal or a written warning.
    b. For major infractions, with the definition of "major" to be determined by the Data Security Coordinator or board of directors based upon the nature of the violation and the nature of the Personal Information affected by the violation, the employee or Board Member shall be disciplined by suspension or termination. The definition of "major" may include a pattern of three or more "minor" violations.
6. Resigned or terminated employees or Board Members must return all records containing Personal Information , in any form, that may be in the former employee's or Board Member's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
7. A resigned or terminated employee's or Board Member's physical and electronic access to Personal Information must be immediately blocked. Such resigned or terminated employee or Board Member shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the Corporation's premises or information. Moreover, such terminated employee's or Board Member's remote access to Personal Information (such as internet access, e-mail access, voice-mail access) must be disabled. The Data Security Coordinator shall maintain a highly secured master list of all lock combinations, passwords and keys.
8. Employees and the members of the Corporation's board of directors are encouraged to report any suspicious or unauthorized use of Personal Information.

III. PROTECTIONS AGAINST EXTERNAL DATA SECURITY BREACH

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 are effective immediately:

A. The Corporation's Office:

1. The Corporation's office is intended to be a secure facility, due to the Personal Information contained in the Corporation's files. All paper records containing Personal Information shall be maintained in locked storage when the office is unoccupied.
2. Visitors shall not be permitted to visit unescorted any area within the Corporation's office that contains Personal Information.
3. The Corporation's office shall be locked at all times when unoccupied.

B. Third Party Service Providers

1. "Third Party Service Providers" are defined as any non-employee to whom the Corporation grants partial or full access to the Corporation's paper or electronic data that contains Personal Information or to areas within the Corporation's office in which Personal Information is stored.
2. All Third Party Service Providers must acknowledge in writing that they have instituted Personal Information security measures and their business operations are in compliance with the requirements of CMR 17.00 as it relates to Personal Information to which the Corporation has granted them access.
3. The Data Security Coordinator shall maintain all Third Party Service Providers acknowledgments.

C. The Corporation's Computers and Electronic Information Systems

1. The wireless network at the Corporation shall always be encrypted.

2. All laptops used by Corporation personnel must be password protected.

3. All portable devices used by employees or Board Members of the Corporation to send and receive their Corporation e-mail shall be password protected, and shall be locked when not in use.

4. The Corporation's computers and computer system, including any wireless system, shall, at a minimum, and to the extent technically feasible, have the following elements:

a. Secure user authentication protocols including:

   i. control of user IDs and other identifiers;
   ii. a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
   iii. 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;
   iv. restricting access to active users and active user accounts only; and
   v. blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

b. Secure access control measures that:

   i. restrict access to records and files containing Personal Information to those who need such information to perform their job duties; and
   ii. assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

c. Encryption of all transmitted records and files containing Personal Information that will travel across public networks, and encryption of all data containing Personal Information to be transmitted wirelessly.

d. Reasonable monitoring of systems, for unauthorized use of or access to Personal Information;

e. Encryption of all Personal Information stored on laptops or other portable devices;

f. For files containing Personal Information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Personal Information.

g. Reasonably up-to-date versions of system security agent software installed and active at all times, which must include

anti-virus, anti-spyware, and anti-malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

D. Personal Information Removed from the Corporation

1. Employees and Board Members shall only remove paper or electronic Personal Information from the Corporation when they have a legitimate and authorized business purpose for removing such information and only with prior authorization of the Executive Director.
2. Any employee or Board Member of the Corporation removing electronic Personal Information from the Corporation office shall only do so on a secure device, such as an encrypted laptop or encrypted USB drive.
3. Any employee or Board Member who removes Personal Information from the Corporation must keep the Personal Information secured. The measures taken to secure such Personal Information shall include whatever is necessary to secure the information from unauthorized use or access in the environment in which the employee or Board Member must use the information for their legitimate business purpose.
4. Any employee or Board Member who experiences a data security breach relating to Personal Information removed from the Corporation shall immediately inform the Data Security Coordinator.

IV. PERSONAL INFORMATION SECURITY BREACH

A. Employees and members of the board of directors must notify the Data Security Coordinator in the event of a known or suspected Personal Information security breach or unauthorized use of Personal Information.

B. The Corporation shall provide notice as soon as practicable and without unreasonable delay when the Corporation (a) knows or has reason to know of a Personal Information security breach, or (b) knows or has reason to know that the Personal Information of a Massachusetts resident was acquired or used by an unauthorized person or used for an unauthorized purpose. The following notices shall be issued:

1. Notice shall be provided to the Massachusetts resident whose information was acquired or otherwise affected by an unauthorized person. Such notice shall include the nature of the breach of security or unauthorized acquisition or use, and any steps the Corporation has taken or plans to take relating to the incident.

2. To the extent required by M.G.L. c. 93H,§3, notice shall be provided to the Massachusetts Attorney General and to the Massachusetts Director of Consumer Affairs and Business regulation. Such notice shall include the nature of the breach of security or unauthorized acquisition or use, the number of residents of Massachusetts affected by such incident at the time of notification, and any steps the Corporation has taken or plans to take relating to the incident.

C. Whenever there is a Personal Information security breach or unauthorized use of Personal Information, 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 Corporation's security practices are required to improve the security of Personal Information for which the Corporation is responsible.

_____, INC.

ACKNOWLEDGEMENT AND CERTIFICATION

(Employees and Board Members)

I hereby acknowledge that I have received a copy of the Corporation's Written Information Security Program (WISP) and certify that I will comply with the provisions of the Corporation's Written Information Security Program and related policies, procedures, standards and guidelines.

I acknowledge that if I have any questions regarding the Corporation's WISP or related policies, procedures, standards or guidelines, it is my responsibility to address those issues with the Corporation's Data Security Coordinator for clarification.

I acknowledge that failure on my part to practice due care and due diligence with respect to Personal Information and the Corporation's WISP may result in the termination of my employment or board of directors service for cause.

The terms of this acknowledgement shall survive any termination of employment or board of directors service.

_____

NAME (PRINTED)

_____

SIGNATURE

Date: _____ , 20___

_____, INC.

ACKNOWLEDGEMENT AND CERTIFICATION

(Third Party Service Providers)

I hereby certify that my company has instituted (if I am not part of a company, that I have instituted) Personal Information security measures in compliance with Massachusetts General Laws c. 93H and 201 Code of Mass. Regulations 17.00, and that my company's business operations (my business operations, if I am not part of a company) are in compliance with these legal requirements with respect to Personal Information to which the client Corporation has granted my company access (has granted me access, if I am not part of a company).

I acknowledge that if I have any questions regarding the Corporation's WISP or related policies, procedures, standards or guidelines, it is my responsibility to address those issues with the Corporation's Data Security Coordinator for clarification.

I acknowledge that failure on my part to practice due care and due diligence with respect to Personal Information and the Corporation's WISP may result in the termination of my (and my company's) service arrangement with the Corporation for cause.

The terms of this acknowledgement shall survive any termination of service.

_____

NAME (PRINTED)

_____

COMPANY NAME (PRINTED)

_____

SIGNATURE

Date: _____ , 20___