STEPS TO SUCCESS, INC.

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

I. GENERAL

A. Objective of WISP

This Written Information Security Program ("***WISP***") sets forth the practices and procedures used by Steps to Success, Inc. ("***STS***") to safeguard any Personal Information contained in paper or electronic records in the possession of STS, all in compliance with STS's obligations under M.G.L. c. 93H, M.G.L. c. 93I, and 201 CMR 17.00. These safeguards are designed and intended to:

1. ensure the security and confidentiality of Personal Information of any resident of Massachusetts;

2. protect against threats or hazards to the security or integrity of such Personal Information; and

3. protect against unauthorized access to or use of such Personal Information in a manner that creates a substantial risk of identity theft or fraud.

B. Personal Information

"***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; or

(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).

C. Scope of WISP

In formulating and implementing STS'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

STS has designated the then-current Executive Director to be STS's Data Security Coordinator. She will be responsible for implementing, supervising and maintaining STS's WISP, including:

1. initial implementation of STS's WISP;

2. training of the following persons regarding STS's WISP and Personal Information security:

(a) all employees;

(b) Members of the STS Board of Directors with access to Personal Information ("***Board Member(s)***");

(c) independent contractors with access to Personal Information; and

(d) any other person involved with STS who has or will have access to Personal Information.

3. regular testing of the WISP's safeguards;

4. evaluating the ability of each of STS's third party service providers to implement and maintain appropriate Personal Information security measures for the Personal Information to which STS has permitted them access and requiring such third party service providers to implement and maintain appropriate Personal Information security measures;

5. reviewing the security measures in the WISP at least annually, or whenever there is a material change in STS's business practices that may implicate the security or integrity of records containing Personal Information, including apprising the

Board of Directors of the results of that review and any recommendations for improved security arising out of that review.

E. Limits on Collection and Storage of Personal Information at STS

1. As an employer, STS may possess Personal Information for its employees. The Personal Information that is collected and stored from each employee shall be limited to that information which is (i) necessary for employment, such as tax forms, (ii) voluntarily provided to obtain certain benefits of employment, such as pension, health, life and disability insurances, or (iii) necessary for STS to comply with state or federal laws and regulations.

2. As part of its legitimate organizational purpose, STS may possess Personal Information of Massachusetts residents obtained during the course of STS's activities. The Personal Information that is collected and stored shall be limited to that information which is (i) reasonably necessary to accomplish STS's legitimate organizational purpose, or (ii) necessary for STS to comply with state or federal laws and regulations.

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 STS's legitimate business purposes, or necessary for STS 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 STS's legitimate business purposes or to enable STS 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 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. As a condition of their employment or Board service, all employees and Board Members must sign an Acknowledgement and Certification (attached hereto as Exhibits 1 and 2) that they have received a copy of STS's WISP and that they will comply with the provisions of the WISP. These signed acknowledgements and certifications shall be retained by STS.

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.

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, STS shall implement the following disciplinary procedure:

(a) For minor infractions, with the definition of "minor" to be determined by the Executive Director 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 Executive Director 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 employees 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 STS'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. STS shall maintain a highly secured master list of all lock combinations, passwords and keys.

8. Employees and the members of STS's Board of Directors are encouraged to report any suspicious or unauthorized use of Personal Information.

III. PROTECTIONS AGAINST EXTERNAL DATA SECURITY BREACH

STS will implement the following measures in order 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.

A. STS's Office

1. STS's office is intended to be a secure facility, due to the Personal Information contained in STS's files. All paper records containing Personal Information shall be maintained in a locked file cabinet when the office is unoccupied.

2. Visitors shall not be permitted to visit unescorted any area within STS's office that contains Personal Information.

3. STS'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 STS grants partial or full access to STS's paper or electronic data that contains Personal Information or to areas within STS's office in which Personal Information is stored.

2. All Third Party Service Providers must acknowledge in writing (in substantially the same form set forth as Exhibit 3 hereto) 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 STS has granted them access.

C. STS's Computers and Electronic Information Systems

1. The wireless network at STS 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 STS to send and receive their Corporation e-mail shall be password protected, and shall be locked when not in use.

4. STS'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 STS

1. Employees and Board Members shall only remove paper or electronic Personal Information from STS 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 STS removing electronic Personal Information from STS 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 STS 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 STS shall immediately inform the Data Security Coordinator.

IV. PERSONAL INFORMATION SECURITY BREACH

A. Employees and Board Members 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. STS shall provide notice as soon as practicable and without unreasonable delay when STS (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 by the Executive Director:

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 STS 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 STS 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 STS's security practices are required to improve the security of Personal Information for which STS is responsible.