infinity Benefit Foundation

INFINITY BENEFIT FOUNDATION, INC.
COMPREHENSIVE INFORMATION SECURITY POLICY

I. OBJECTIVE

It is the objective of Infinity Benefit Foundation, Inc. ("IBF") in the development and implementation of this Comprehensive Information Security Policy ("CISP") to create effective administrative, technical and physical safeguards for the protection of personal information. This CISP sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information. For purposes of this CISP, "personal information" means an individual'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 individual: (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 an individual'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. IBF generally acquires personal information in connection with hiring employees and payroll, enlisting volunteers, accepting donations from members of the public and enabling donors to establish donor advised fund accounts.

II. PURPOSE

The purpose of the CISP is to:

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

III. DATA SECURITY COORDINATOR

IBF appoints _____ to be its Data Security Coordinator. The Data Security Coordinator will be responsible for:

- Initial implementation of the CISP;
- Regular testing of the CISP's safeguards;
- Evaluating the ability of each of IBF's third party service providers to implement and maintain appropriate security measures for the personal information to which IBF permits them access, and requiring such third party service providers to implement and maintain appropriate security measures;
- Reviewing the scope of the security measures in the CISP at least annually, or whenever there is a material change in IBF's business practices that may implicate the security or integrity of records containing personal information; and
- Conducting an annual training session for all directors, officers, employees, volunteers, and independent contractors, including temporary and contract employees who have access to personal information on the elements of the CISP.

IV. HANDLING PERSONAL INFORMATION

A. Electronically Held Records

IBF requires the following security systems with respect to the maintenance of personal information on its computers:

Authentication Protocols. The Data Security Coordinator shall secure user authentication protocols including:

- Control of user IDs and other identifiers;
- A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
- 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;
- Restricting access to active users and active user accounts only; and
- Blocking access to user identification after multiple unsuccessful attempts to gain access.

Access Protocols. The Data Security Coordinator shall implement the following secure access control measures:

- Restrict access to records and files containing personal information to those who need such information to perform their job duties; and

- Assign to each person with computer access unique identifications plus passwords, which are not vendor supplied default passwords, and which are reasonably designed to maintain the integrity of the security of the access controls.

Restriction on E-mailing Personal Information. IBF will not, as a general rule, send or accept personal information by e-mail. To the extent exceptions must be made, the security measures described in this CISP shall be taken.

Encryption. Should any records and files containing personal information be transmitted across public networks or wirelessly, such records or files shall be encrypted. Personal information stored on laptops and other portable devices shall also be encrypted.

Monitoring. IBF shall take all steps necessary to reasonably monitor its computer network for unauthorized use of or access to personal information.

Firewalls. All files containing personal information on a system that is connected to the Internet shall be protected by reasonably up-to-date firewall protection and operating system security patches designed to maintain the integrity of the personal information.

Virus protection. All computers containing personal information shall be protected by reasonably up-to-date versions of system security software, including malware protection and reasonably up-to-date patches.

B. Paper Records

In the ordinary course of business, all of IBF's records containing personal information are held electronically. In the event personal information is obtained in paper copy, IBF will keep such paper records in a locked file cabinet with restricted access, and will destroy such records regularly in accordance with IBF's document destruction policy using an office-grade shredder. Paper records containing personal information will not be permitted to be taken out of the office and will be accessible only by personnel with a business necessity.

If IBF receives a paper check from a donor, it will make only one hard copy and keep it in a locked file cabinet with restricted access. The check itself will also be kept under lock and key until deposited.

V. TRAINING

The Data Security Coordinator shall ensure that all employees, whether full-time, part-time, seasonal or temporary, and independent contractors, consultants, volunteers and interns who have access to personal information are trained on the data security requirements provided in this CISP.

VI. PERSONS SEPARATING FROM IBF

All employees, whether full-time, part-time, seasonal or temporary, and independent contractors, consultants, and volunteers, upon termination or resignation, shall immediately be denied access to physical and electronic records containing personal information and will be required to return or destroy all records and files containing personal information in any form that may at the time of such termination or resignation be in their possession or control, including all such information stored on laptops, portable devices, or other media, or in files, records, notes, or papers.

VII. SECURITY BREACH AND NOTIFICATION

All employees, whether full-time, part-time, seasonal or temporary, and independent contractors, consultants, and volunteers shall as soon as practicable and without unreasonable delay notify the Data Security Coordinator when such person knows or has reason to know of a security breach or when the person knows or has reason to know that personal information was acquired or used by an unauthorized person or used for an unauthorized purpose.

A "security breach" is any unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information that creates a substantial risk of identity theft or fraud. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for lawful purposes, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

When the Data Security Coordinator is informed of a security breach, he/she will (1) notify the individual whose information was compromised, and (2) notify the relevant authorities. In Massachusetts, the relevant authorities are the Attorney General and the Office of Consumer

Affairs and Business Regulation. Security breaches involving personal information of residents of other states and countries will be handled in accordance with the requirements of such jurisdictions.

The notice to the individual will be in writing, possibly by electronic mail, and will include the following information:

- Identification of the personal information that may be at risk;
- A description of IBF's security program;
- The individual's right to obtain a police report;
- Suggestion of extra caution, to review account statements, and to obtain a credit report;
- How to request a security freeze;
- The necessary information to be provided when requesting the security freeze;
- Any fees to be paid to any of the consumer reporting agencies; and
- A phone number to call within IBF for further information.

The notification to the individual shall not include a description of the nature of the breach or unauthorized acquisition or use or the number of people affected by the security breach or unauthorized access or use.

The notice will not be provided if law enforcement personnel advise against it. In Massachusetts, notice to the Office of Consumer Affairs and Business Regulation and to the Attorney General will include the following:

- A detailed description of the nature and circumstances of the breach of security;
- The number of people affected as of the time of notification;
- The steps already taken relative to the incident;
- Any steps intended to be taken relative to the incident subsequent to notification; and
- Information regarding whether law enforcement is investigating the incident.

Non-Retaliation. IBF will not retaliate against anyone who reports a security breach or non-compliance with CISP, or who cooperates in an investigation regarding such breach or non-compliance. Any such retaliation will result in disciplinary action by IBF up to and including suspension or termination.

Documentation. IBF shall document all responsive actions taken in connection with any incident involving a security breach.