Adopted on: June 4, 2022

Resolve New England, Inc.

Comprehensive Written Information Security Program (WISP)

I. Objective

The objective of this Written Information Security Program (hereinafter "WISP") is to create technical and physical safeguards for the protection of the Personal Information (hereinafter "PI") held by Resolve New England, Inc. (hereinafter "RNE").

II. Purpose

This WISP is adopted in conformity with the Massachusetts data security law, G.L. c. 93H, and its accompanying regulations, 201 C.M.R. 17.00. The Massachusetts Office of Consumer Affairs and Business Regulation (hereinafter "OCABR") has issued 201 C.M.R. 17.00 to help organizations comply with their legal obligations. This WISP is intended to prepare RNE to meet the standard put forth by the OCABR.

The goals of this WISP are to:

i. Identify PI pursuant to Massachusetts law and confidential information as defined by RNE.

ii. Ensure the security and confidentiality of both PI and other confidential information as defined by RNE and protect the legal rights of its board members, organization members, supporters and any other applicable persons.

iii. Protect RNE against anticipated threats or hazards to said information.

iv. Decrease the level of unanticipated risk to the PI held by RNE.

v. Protect RNE against unauthorized access to or use of said information in a manner that decreases the risk of identity theft or fraud.

III. Scope and Definitions

The standards defined herein are designed to minimize the potential exposure of RNE from damages associated with the unauthorized use of its resources. Damages include, but are not limited to, the loss of sensitive, personal, or confidential data, damage critical to RNE's computer resource networking systems, and damage to reputation. The scope of this WISP most specifically pertains to the following set of data and systems.

Personal Information is defined as being a Massachusetts resident's first name and last name or first initial and last name in conjunction with one or more of the following data elements that relate to said individual:

i. Personal identification
   - Social Security Number
   - State ID card
   - Driver's license number
   - Passport information
   - Employee ID

ii. Financial account information
   - Bank account numbers
   - Credit or debit card numbers

iii. Other ID information granting access to financial accounts or non-public records
   - Usernames
   - Passwords
   - PINs

Provided, however, that PI 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 (*e.g.,* real estate records and lawsuit filing records; birth, marriage and divorce records; motor vehicle data). The disposal of PI must be done in a manner so that it may not be practicably read or reconstructed (see Addendum F).

Though this policy is developed in conformity with Massachusetts law, any personal information collected by RNE about non-Massachusetts residents is also handled with the same utmost care described herein.

Confidential Information is defined as any non-public information owned or licensed by RNE including but not limited to:

> board members, organization members, supporters and any other applicable persons' correspondence; RNE's private communications and strategies; lists, business plans, services, payment, items, specifications, documentations, rules and procedures; technical and other data; contracts; and databases.

Computer Resources and Information Systems are the property of RNE and are intended to be used for servicing the interests of RNE, and of RNE's clients, visitors, personnel, members, directors, officers, donors, and other applicable persons in the course of normal operations.

i. Computer Resources are to include all Internet/Intranet/Extranet-related systems, including but not limited to computer equipment (owned or leased by RNE), software, operating systems, storage, media, websites, network accounts providing electronic mail, Internet browsing, and FTP.

ii. Information Systems are to include any technology or electronic device that stores data for the purpose of allowing access to said data.

Terms and Definitions hereinafter used within the text of this WISP and related policies and procedures, unless noted otherwise, shall have the following meanings:

i. **Breach of security** shall be defined as the unauthorized acquisition or use of unencrypted or encrypted electronic data and key / password / access that is capable of compromising the security, confidentiality, or integrity of PI, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth. A good faith but unauthorized acquisition of PI by a person or agency, or employee of agent thereof, for the lawful purpose of such person or agency, is not a breach of security unless the PI is used in an unauthorized manner or subject to further unauthorized disclosure.

ii. **Electronic** shall be defined as relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capacities.

iii. **Electronic records** shall be defined as any combination of text, graphics, data, audio, pictorial or information in digital form created, modified, maintained, archived, retrieved or distributed by a computer system.

iv. **Encryption** shall be defined as the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

v. **Internet** shall be defined as a global system of interconnected computer networks that are linked by a myriad of electronic and optical networking technologies.

vi. **Owns or licenses** shall be defined as receiving, storing, maintaining, processing, or otherwise having access to PI in connection with the provision of goods and services.

vii. **Person** shall be defined as a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth of Massachusetts, or any of its branches, or any political subdivision thereof.

viii. **Record** shall be defined as any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

ix. **Third-party** shall be defined as any person that receives, stores, maintains, processes, or otherwise is permitted access to personal or confidential information through its provision of service directly to the Corporation.

IV. Roles and Responsibilities

Cohesive and active participation of every volunteer and affiliate of RNE whom deals with information or information systems is necessary in order to implement an effective information security program that maximizes the performance of RNE. **It is the responsibility of said individuals to know these guidelines and to conduct their activities accordingly.**

Furthermore, all Third-party service providers who have, or are responsible for personal or confidential information in physical or electronic form must comply with this program.

Data Security Coordinator: RNE has designated Emily Lindblad, Operations Manager, to implement, supervise and maintain the WISP. Emily will be responsible for:

i. Initial implementation of the WISP;

ii. Monitoring RNE's operation and practices that handle PI and ensuring all PI that RNE receives and maintains shall be safeguarded in compliance with Massachusetts law.

iii. Regular testing of the WISP's safeguards;

iv. Evaluating the ability of each of RNE's third-party service providers to implement and maintain appropriate security measures for the PI to which RNE has permitted them access and requiring said third-party service providers by contract to implement and maintain appropriate security measures.

v. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in RNE's business practices that may implicate the security or integrity of records containing PI.

vi. Ensuring that the amount of PI collected is limited to that amount reasonably necessary to accomplish RNE's legitimate business purposes or necessary to comply with other state or federal regulations.

vii. Conducting an immediate, mandatory post-incident review if there is an incident that requires notification under M.G.L. c. 93H, §3. The review will assess events and actions taken, if any, with a view to determining whether any changes in RNE's security practices are required to improve the security of PI for which RNE is responsible.

Third Parties: Every contractor, consultant, service provider including fundraising portals and payroll vendors (hereinafter "Third Parties") who must have access to personal or confidential information or to computer resources and information systems as part of the service said Third Parties provide must comply with the provisions of this WISP.

i. Access to personal or confidential information by Third Parties is on a "need-to-know" basis as identified by the Data Security Coordinator or management team.

ii. Third Parties with access to RNE's personal or confidential information or computer resources and information systems must agree in writing that their own Information Security Programs conform with Massachusetts regulation 201 CMR 17.03(2)(f)2. See attached certification form.

V. Internal Risk

In order to combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, RNE has adopted procedures set forth in the attachment to this document.

VI. External Risk

In order to combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PI, and evaluating and improving

the effectiveness of the current safeguards for limiting such risks, RNE has adopted procedures set forth in the attachment to this document.

VII. Monitoring, Enforcement and Breach of Security

Monitoring:

It is the responsibility of the Data Security Coordinator to monitor the WISP and associated policies so to ensure said program and policies are operating in a manner reasonably calculated to prevent unauthorized access to, or unauthorized use of personal and confidential information, and, further, to ensure Personnel and third-party compliance with these procedures.

Enforcement:

Failure on the part of Third Parties to follow this program and its associated policies may subject RNE to action by the Massachusetts Attorney General, under Massachusetts General Laws, which could potentially include: (1) injunctive relief; (2) civil penalties of not more than $5,000 for each violation; (3) costs of investigation and litigation, possibly including attorney's fees. A party may be held liable under civil law for any breach or increased duty of care. Additionally, failure to adhere to all applicable regulations pertaining to proper disposal of sensitive records may result in fines of up to $100 per person affected, but not to exceed $50,000 for each instance of improper disposal.

Notification of Breach of Security:

i. Should a PI data breach occur, the Data Security Coordinator is required to notify the Massachusetts OCABR, the Massachusetts Attorney General's Office, each Massachusetts resident who has had any PI kept by RNE, as well as any other applicable entity(ies).

ii. If RNE knows or has reason to know of PI data breach, RNE is required to provide written notice to the Massachusetts Attorney General, the Massachusetts OCABR, as well as affected Massachusetts residents as soon as practicable and without unreasonable delay (see RNE's WISP Procedures).

Written notices to the Massachusetts Attorney General and to the Director of OCABR shall include: (1) the nature of the breach of security or the unauthorized acquisition or use; (2) the number of Massachusetts residents affected by said incident at the time of notification; (3) any and all measures taken by RNE relating to said breach of security.; (4) the name of the person responsible for the breach; and (5) whether RNE maintains a WISP.

Notice to those affected Massachusetts residents shall include: (1) the consumer's right to obtain a police report; (2) the method the consumer can use to request a

security freeze; (3) the necessary information to be provided when requesting the security freeze and (4) that such freeze will be provided at no charge; provided however, that the notification shall not include:

i. The nature of the breach or unauthorized acquisition or use; or

ii. The number of Massachusetts residents affected by the security breach or the unauthorized access or use.

If breach includes a social security number, RNE shall contract with a third-party to offer to each resident whose social security number was disclosed in the breach of security or is reasonably believed to have been disclosed in the breach of security, credit monitoring services at no cost to said resident for a period of not less than 18 months. RNE shall provide all information necessary for the resident to enroll in credit monitoring services and shall include information on how the resident may place a security freeze on the resident's consumer credit report.

RNE shall not require a resident to waive the resident's right to a private right of action as a condition of the offer of credit monitoring services.