Comprehensive Written Information Security Program (WISP)

Adopted 2021-06-16.

Objective

The objective of developing and subsequently implementing this Comprehensive Written Information Security Program (hereinafter “WISP”), is to create and when necessary, build upon preexisting administrative, technical and physical safeguards for the protection of the Personal Information (“PI”) held by Freedom of Form Foundation, Inc. (“the Organization”). This WISP outlines an effective policy with supporting procedures for the protection of PI in compliance with Massachusetts law, as well as all practicable business best practices regardless of jurisdiction.

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 the Organization to meet the standard put forth by the OCABR.

The goals of this WISP are to:

1. Identify PI pursuant to Massachusetts law and confidential information as defined by the Organization.
2. Ensure the security and confidentiality of both PI and other confidential information as defined by the Organization and protect the legal rights of board members, organization members, supporters, and any other applicable persons.
3. Protect said information pertaining to the Organization, its board members, organization members, supporters, and any other applicable persons, against anticipated threats or hazards.
4. Decrease the level of unanticipated risk to the PI held by the Organization.
5. Protect against unauthorized access to or use of said information, in a manner that decreases the risk of identity theft or fraud.

Scope and Definitions

The standards defined herein are designed to minimize the potential exposure of the Organization 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 the Organization’s computer resource networking systems, intellectual property, and damage to reputation. The scope of this WISP most specifically pertains to the following set of data and systems.

Personal Information (PI)
Personal Information is defined as being a person’s first name and last name or first initial and last name (especially for Massachusetts residents in conformity with G.L. c.93H, though

residents of other jurisdictions will be treated similarly by the Organization to the maximum extent practicable) *in conjunction with* one or more of the following data elements that relate to said individual:

1. Personal identification
    a. Social Security Number
    b. State ID card
    c. Driver's license number
    d. Passport information
    e. Employee ID
2. Financial account information
    a. Bank account numbers
    b. Credit or debit card numbers
3. Other ID information granting access to financial accounts or non-public records
    a. Usernames
    b. Passwords
    c. PINs
4. Employee records
    a. Payroll
    b. Pension
    c. Insurance

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 Procedure G).

Confidential Information (CI)
Confidential Information is defined as any non-public information owned or licensed by the Organization including but not limited to:

1. Director/officer/personnel/member/ donor/consultant/and any other applicable person correspondence;
2. Organization private communications and strategies;
3. Lists, business plans, services, payment, items, specifications, documentations, rules and procedures;
4. Technical and other data;
5. Contracts;
6. Intellectual property, presentations, business methods, analyses, plans, databases, formats, methodologies, applications, developments, inventions, processes, designs, drawings, algorithms, and delivery and inspection procedures;
7. Marketing strategies or initiatives; and
8. Financial plans or records.

Computer Resources and Information Systems

Computer Resources and Information Systems are the property of the Organization and are intended to be used for servicing the interests of the Organization, and of said Organization's director/officer/personnel/member/donors, and other applicable persons in the course of normal operations.

1. Computer Resources are to include all Internet/Intranet/Extranet- related systems, including but not limited to computer equipment (owned or leased by the Organization), software, operating systems, storage, media, websites, network accounts providing electronic mail, Internet browsing, and file transfer protocols (FTPs).
2. 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

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

1. **Breach of PI Security** shall be defined as the 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 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 PI Security unless the PI is used in an unauthorized manner or subject to further unauthorized disclosure.
2. **Breach of CI Security** shall be defined as the 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 company CI. Note this is not mutually exclusive with Breach of PI Security.
3. **Electronic** shall be defined as relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capacities.
4. **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.
5. **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.
6. **Extranet** shall be defined as a private network that uses Internet technology and the public telecommunication system to securely share part of the Organization's information or operations with suppliers, vendors, partners, or other businesses.
7. **Internet** shall be defined as a global system of interconnected computer networks that are linked by a myriad of electronic and optical networking technologies.
8. **Intranet** shall be defined as a private network that is contained within the Organization's enterprise.
9. **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 or in connection with employment.

10. **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.
11. **Personnel** shall be defined as any employee, temporary employee, volunteer, or board members of the Organization who have access to PI or CI.
12. **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.
13. **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 Organization. For further definition, see *Roles and Responsibilities -> Third Parties*.
14. **Company Record Access Credentials** shall be defined as User IDs, passwords, two-factor authentication tokens, secondary email accounts used to reset or recover passwords, and related components of securely accessing Electronic Records, as well as lock/key combinations such as those used to access any physically secured and locked data or Records.

Roles and Responsibilities

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

Furthermore, all Personnel and 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
The Organization has designated Ramon Reyes to act as the Data Security Coordinator in order to implement, supervise and maintain the WISP. Ramon Reyes will be responsible for:

1. Initial implementation of the WISP;
2. Conducting an annual training session for all Personnel, members, managers, and independent contractors, including temporary and contract employees who have access to PI on the elements of the WISP. All attendees at said training sessions are required to certify their attendance at the training, and their familiarity with the Organization's requirements for ensuring the protection of PI.
3. Regular testing of the WISP's safeguards;
4. Evaluating the ability of each of the Organization's third-party service providers to implement and maintain appropriate security measures for the PI to which the

Organization has permitted them access and requiring said third-party service providers by contract to implement and maintain appropriate security measures.

5. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in the Organization's business practices that may implicate the security or integrity of records containing PI.
6. Ensuring that Organization Personnel change computer IDs and passwords periodically.
7. Ensuring in coordination with Personnel in charge of departments and programs all Company Record Access Credentials used to access or work with PI or CI are secure and used in compliance with this WISP and policies.
8. Maintaining a highly secure master list of all Company Record Access Credentials used to access or work with PI or CI, or ensuring that the head of each department / program maintains a highly secure master list of Company Record Access Credentials under their supervision to access or work with PI or CI.
9. Ensuring that, in the event that an employee is terminated, the former employee's remote electronic access to PI is immediately disabled, and the former employee's voicemail access, e-mail access, internet access, and passwords are invalidated.
10. Ensuring that the amount of PI collected is limited to that amount reasonably necessary to accomplish the Organization's legitimate business purposes or necessary to comply with other state or federal regulations.
11. 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 the Organization's security practices are required to improve the security of PI for which the Organization is responsible.

Personnel

All Personnel (as defined above) of the Organization must comply with the provisions of this WISP.

1. Access to personal or confidential information by Personnel is on a "need-to-know" basis as identified by the Data Security Coordinator or management team.
2. Personnel must read this WISP and associated policies and procedures as well as document said action by signing the WISP Acknowledgment Form to be retained in Human Resource files.
3. Personnel must receive training provided by the Data Security Coordinator in effective information security practices.
4. Upon termination of any Personnel, physical and electronic access will be blocked immediately. No information in physical or electronic form will be removed from the premises unless specifically reviewed and approved by the Organization management.
5. Terminated employees must return all records containing PI, 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.).
6. The Organization requires its Personnel to immediately report any suspicious or unauthorized use of PI to the Data Security Coordinator.

Third Parties

Every contractor, consultant, service provider including fundraising portals, and vendor (hereinafter "Third Parties") including all Personnel affiliated with 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.

1. 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.
2. Third Parties with access to the Organization's PI, confidential information or computer resources and information systems must agree in writing that their own Information Security Programs conform minimally to the policies and procedures defined herein as they relate to the work defined by their contracts. If necessary, contracts must be amended to conform with Massachusetts regulation 201 CMR 17.03(2)(f)2, which states that a Company must "[o]versee service providers, by… [r]equiring such third-party service providers by contract to implement and maintain such appropriate security measures for PI…".

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, the Organization has adopted procedures set forth later in this document.

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, the Organization has adopted procedures set forth later in this document.

Training

This WISP calls for regular ongoing training for Personnel in the proper management of PI to instill the importance of the security of Personal and Confidential Information. Associated policies in conjunction with all aspects of this WISP shall be regarded as the objective of said training. A further objective is that Personnel understand the ramifications if appropriate information security procedures pursuant to this WISP and applicable Massachusetts General Laws are not followed.

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 Personnel and Third Parties to follow this program and its associated policies may subject organizations 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 PI Security

1. Should a Breach of PI Security 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 the Organization, as well as any other applicable entity(ies).
2. If the Organization is knowledgeable of or has reason to know of a Breach of PI Security, or that PI of Massachusetts residents was acquired by or used by an unauthorized person or entity for an unauthorized purpose, the Organization 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. The Organization will provide similar written notice to residents of other states and other governmental agencies to the fullest extent practicable.

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

1. The nature of the breach or unauthorized acquisition or use; or
2. The number of Massachusetts residents affected by the security breach or the unauthorized access or use.

If the breach includes a social security number, the Organization shall contract with a third party to offer to each resident whose social security number was disclosed in the Breach of PI

Security or is reasonably believed to have been disclosed in the Breach of PI Security, credit monitoring services at no cost to said resident for a period of not less than 18 months. The Organization 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.

The Organization 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.

Procedures

Overview
Freedom of Form Foundation, Inc.'s WISP is Implemented through the following Procedures. The corporation will be referred to hereinafter as the "Organization".

In implementing WISP and its procedures, the Organization shall take the following steps:

1. Assess the need for collecting any information that may contain Personal Information (hereinafter "PI"). Normally this starts with donation checks and employment records.
2. Only collect PI when absolutely necessary.
3. NOT collect any information from individuals unless necessary for the Organization's operation.
4. NOT retain or store any information that includes PI unless necessary for the Organization's operation. This includes not making copies of the documents that contain PI (which action doubles liability exposure)

It is important NOT to collect PI unless necessary so as to minimize the risk exposure to the Organization, and not to create an unnecessary administrative burden.

Procedure A: Protection of Physical Records Containing Personal Information
The Organization seeks to protect any physical records containing PI by ensuring the appropriate and secure storage of, access to, and transportation of said information within the Organization, or with any number of related Third-Party service providers.

The Organization does not presently store physical records containing PI about directors, officers, donors, or other applicable persons.

Any physical, paper files and records will be retained and destroyed pursuant to Procedure G.

Procedure B: Protection of Electronic Records Containing PI
The Organization seeks to protect electronic records which contain PI by identifying and implementing safe procedures for securing the storage of, access to, and transportation of electronic PI within and outside the Organization.

The Organization maintains its electronic records and files on secure servers which are administered by Ramon Reyes (Chief Information Officer) and Daniel Davies (Vice President). PI stored on servers, whether physically on premises or physically located off-site, is fully encrypted on the servers, and remains fully encrypted at all times including during transmission, unless the PI is being read or worked with by authorized persons. When servers are not undergoing maintenance or updates, or are not otherwise under active use by authorized Personnel, the servers are locked, such that they are inaccessible to unescorted and unauthorized persons.

The Organization updates its malware protection, firewall protection, and virus identification on at least a monthly basis. Computer systems are regularly monitored for attempted attacks and for unauthorized use of or access to PI.

PI is only allowed to be stored or cached on a non-server device, such as a laptop, handheld device, or other portable device, if: (1) that device is explicitly declared to both the Chief Information Officer and the Data Security Coordinator, (2) that device is fully encrypted (encryption of specific files shall not be sufficient), (3) that device is logged out when not in use by authorized persons, (4) that device has measures to limit the number of decryption attempts by unauthorized persons, and (5) that device is maintained to the same standard as our secure servers, by keeping malware protection, firewall protection, virus identification, and so forth up to date. The Chief Information Officer and/or the Data Security Coordinator may deny permission to store PI on any non-server device for any reason, including for suspicion that data protection or encryption may not be sufficiently strong.

Company Record Access Credentials, such as those used to decrypt and work with PI, are shared only on a need-to-know basis and are securely stored and transmitted using LastPass Teams or similarly secure methods.

Electronic transmission of director, officer, donor, and other applicable person's PI to service providers is encrypted and sent only through secure network including secure WiFi. Electronic records are retained and destroyed pursuant to Procedure G.

Procedure C: Acceptable Use of the Organization's Computer Resource Systems
All computer resource systems which contain or have access to PI kept by the Organization are to be considered a potential risk to the Organization. As such, all computer systems, including but not limited to, hardware, software, networks, storage media, websites and portable devices are subject to all relevant policies and procedures hereinafter.

PI may only be used by the Organization or select Third Parties for acceptable business purposes, including maintaining PI connected to tax and financial records; contract records; insurance records; and contact information for directors, officers, donors, and other applicable persons. The use of PI by individuals for private interests or inurement is not acceptable, and will be met with decisive disciplinary action.

PI belonging to the Organization's directors, officers, donors, and other applicable persons is securely stored on password protected computers. The Organization and its agents do not email sensitive PI on public Wi-Fi or without encryption which can be only decoded by keys or passwords at both ends of the communication; nor do they post PI or confidential information on social networking platforms.

PI shall *never* be conveyed via unsolicited incoming phone calls or texts. Also, PI shall not be conveyed via *any* phone call or text without explicit permission of the Data Security Coordinator.

Procedure D: User Identification Control
Passwords are to be considered a primary means of reducing many of the aforementioned risks associated with electronic PI protection. Any and all Personnel and Third-Party service providers with direct access to PI, or any computing system holding PI, shall have unique and secure user identifiers.

The Organization's Data Security Coordinator monitors and ensures that computer login IDs and passwords / passphrases are kept secure and confidential by the managers in charge of respective areas of operation. Access to electronically stored PI is limited to those authorized persons having a unique log-in ID, and re-log-in is required when a computer has been inactive for more than a few minutes. The Data Security Coordinator maintains a highly secure list of the system entry points to the Organization's computer and operation systems including the mobile devices, and a separate list of Personnel with access to such entry point to monitor compliance. The computers are password protected and password access is provided only to the Organization's authorized Personnel. Electronic access is blocked after 5 unsuccessful attempts to gain access. The Data Security Coordinator ensures that Organization Personnel change computer IDs and passwords periodically. Passwords/ passphrases are selected to adhere to the best practices recommended by the cyber security industry each year.

Procedure E: Remote Access to PI
This policy seeks to define, and subsequently develop, standards for remote connection to the Organization's electronic systems by Personnel or any Third-Party service provider.

The Organization's mobile devices must be password-protected. The Organization's Personnel are not allowed to use private electronic devices to use or transmit PI pertaining to directors, officers, donors, and other applicable persons of the Organization unless declared to and approved by the Chief Information Officer and Data Security Coordinator according to Procedure B, and a satisfactory plan is in place to remove that access upon termination. The Organization recognizes that the following devices present security risks to PI: laptops; smart phones; personal data assistants (PDAs); hotel, library or other public workstations and Wireless Access Points (WAPs); USB Flash Drives and Memory Cards; CDs; DVDs; and Remote Access Devices (including security hardware). To address the security threats pertaining to these devices, the Organization does the following:

1. Communication or transmission that includes PI must be conducted a device issued or approved by the Organization with all the necessary protections installed. Under no

circumstances, such communication or transmission is conducted on an undeclared or non-approved personal device.

2. Communication or transmission that includes PI must be made through secure modes. Such modes include secure WiFi in conjunction of the use of encryption on both sender's and receiver's ends.

Procedure F: Wireless Communications

The purpose of this policy is to protect the electronic/computer systems of the Organization from wireless communication devices acquiring access to said systems. Only those wireless devices which meet the requirements specified hereinafter shall be granted access to the Organization's electronic/computing systems.

The Organization must monitor what mobile or portable devices are brought into its premises or inside its own firewalls, and what contact they may have with their computer and operation systems. These devices may be the personal properties of the employees, clients, independent contractors, board members, volunteers and visitors. Any such device should be reported to the Data Security Coordinator for security scanning to ensure that it is clear of any malware or virus. The Organization should impress the risk of data breach upon the employees or any agent of the Organization of situations where data transfer may take place using such portable devices.

In addition, the Organization must prohibit employees or any agent who may have access to the Organization's PI from using public Wi-Fi for the work-related communications.

If the Organization's office employs a keycard entry system, it must train the employees or any other agent of the Organization who is issued such card to be aware of data-swiping devices targeting such cards in physical proximity.

Procedure G: Information Retention and Destruction

This policy seeks to address the retention and destruction of all records and documents in physical or electronic form. Further, this policy seeks to comply with federal and state laws and regulations regarding periods of retention for corporate records. Additionally, this policy works to promote efficiency at the Organization.

Records containing PI are to be kept for 7 years after (1) their initial, necessary collection, or (2) after the termination date of the board member, officer, employee, volunteer, or other Personnel, unless those records are, or reasonably likely to become, relevant to litigation, official proceedings, or disputes. Pursuant to Massachusetts law, it is a crime to alter, cover up, falsify, or destroy any document with the intent of impeding or obstructing any official proceeding.
If PI needs to be updated - for example, if a person changes their legal name - this shall be reflected in the history of the Organization's records. Both the original data, and the edited or revised data, shall be on file and traceable until the record's expiration. Updating PI will *not* count as resetting the expiration date.

For example, suppose a volunteer departs the Organization. Their PI shall expire 7 years thereafter. Then, suppose the former volunteer lets us know they changed their name 3

years later. Their PI will be updated in our system, but their PI will still expire on the same timeline: 4 years from that date.

Records that are still deemed essential after that timespan - such as detailing business plans or containing other information valuable for archival purposes - shall be stripped/redacted of PI and preserved. PI redaction shall be to the satisfaction of the Data Security Coordinator.

All other records containing PI shall be, if electronically stored, securely deleted appropriate for the storage medium (e.g. Eraser or SDelete if in magnetic storage), or if stored on paper, shredded to P-3 standards or greater in accordance with DIN66399.

Backups of all records shall be retained to guard against data loss or accidental or unauthorized deletion, and such backups will be retained to the same level of security as the original data. Backups containing PI shall expire when the original records containing that PI expire. Destruction or deletion of backup records will be held to the same standard as the originals.

If a vendor is being hired to destroy records, the Organization will ensure the vendor can provide the Organization with a certificate of destruction, a document containing detailed information about the destruction of the papers that ensures the shredding process complied with all relevant security laws. These certificates help protect the Organization in case of legal action or an audit.

Procedure H: Email and Messaging Retention and Destruction
Emails and messages, collected with consent, that do not contain PI may be preserved for as long as they are deemed useful to the Organization. Notice and means of gathering consent in accordance with Procedure H shall be implemented in all applicable communication mediums.

Procedure I: Website Security and Privacy
The purpose of this policy is to develop a definition of appropriate security and protection of PI collected on the Organization's website. This Procedure I shall be implemented in the form of a Privacy Policy on the Organization's website.

If the Organization's website collects PI, such PI will be gathered only from consenting visitors, and collection and transmission of that PI will be encrypted and secure. PI collected will be the minimum necessary for the intended business purpose.

If the Organization's website is intended to use cookies, such as to collect analytics data or to set user preferences, such cookies will only be used with the visitor's explicit consent.