Volunteer Lawyers Project of the Boston Bar Association

Written Information Security Plan
Policy and Procedures

Effective March 1, 2010
Revised May 20th, 2022

I. Background

Volunteer Lawyers Project of the Boston Bar Association (VLP) has developed this comprehensive Written Information Security Plan ("WISP") to comply with the organization's obligations under 201 CMR 17.00. This WISP sets forth our procedures for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting personal information of residents of the Commonwealth of Massachusetts, and constitutes VLP's Written Information Security Plan as required by state law and regulations.

VLP is committed to protecting the personal information it maintains of its employees and clients.

II. Purpose

The purpose of this WISP is to establish the guiding principles to safeguard Personal Information maintained by Volunteer Lawyers Project in paper, electronic or any other formats. This WISP is designed to protect against reasonably anticipatable threats or hazards to the security or integrity of Personal Information and against unauthorized access to Personal Information in a manner that creates a substantial risk of identity theft or fraud.

For the purposes of this policy, "Personal Information" includes: a Massachusetts resident's first name and last name or first initial and last name, in combination with any one or more of the following data elements:

- Social security number;
- Driver's license number or state-issued identification card;
- Financial account number, or credit 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; or
- Personally identifiable health information.

"Personal Information" does 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.

III. Scope

This policy applies to all VLP employees, independent contractors, consultants, temporary employees, volunteers, students and other workers ("Covered Persons") that have access to personal information obtained by VLP. This policy applies to all Personal Information maintained by VLP in electronic, paper or other formats.

Each Covered Person is responsible for following all procedures and practices regarding the protection of Personal Information and participating in incident management, risk assessments, work processes, and control mechanisms that support the policy.

Employees in designated roles have been assigned specific responsibilities for the deployment, implementation, and maintenance of this WISP policy. These roles and responsibilities are as follows:

WISP Managers: April Jones, Director of Finance and Operations, 857-320-6440, ajones@vlpnet.org. Barbara Siegel, Director of Compliance and Technology, 857-320-6447, bsiegel@vlpnet.org.

Role: The WISP Managers are responsible for the overall implementation and execution of this WISP policy. All questions, issues, and concerns related to this policy should be directed to the WISP Managers. Their work is overseen by Barbara Siegel, Director of Compliance and Technology, 857-320-6447, bsiegel@vlpnet.org.

IV. Risk Assessment

The WISP Managers and other management staff (Executive Director, Deputy Director, and Legal Director) shall meet quarterly to (i) discuss, identify and assess the reasonably foreseeable internal and external risks to the personal information maintained in any of VLP's electronic, paper or other records and (ii) evaluate and improve, where necessary, the effectiveness of the current safeguards in place to limit any such risks. Evaluation shall be ongoing and shall include, but not be limited to:

- Ongoing employee training (including temporary and contract employee training);
- Ensuring employee compliance with policies and procedures set forth herein; and
- Establishing a means for detecting and preventing security system failures

WISP Managers shall perform an annual audit to identify the records, computing system and all storage media used to store personal information and report to the Deputy Director with recommendations for implementation of the policy.

V. Personal Information Handling

A. Information Collection

Only personal information that is pertinent to carrying out the purpose of VLP's business, decisions made in the course of employment, or required by law is collected. Any personal information collected by VLP must be necessary and relevant, and obtained and maintained using methods which respect the individual's right to privacy as well as applicable laws and regulations.

B. Access

All Covered Persons who are required to access Personal Information are responsible for protecting such information from inappropriate disclosure, modification, misuse or loss.

Access to Personal Information shall be limited to those persons who are reasonably required to know such information in order to accomplish VLP's legitimate business or to comply with federal, state or local requirements or regulations.

Access to electronic Personal Information shall be restricted to active users who are required to access said information using active user accounts only.

Terminated or resigned Covered Persons shall be required to immediately return all VLP equipment including handheld devices, notebook computers, keys, identification badges, access codes or badges, business cards and any other property or codes that permit such individual to access VLP's premises or information.

All passwords and information that the individual maintained in order to have access to VLP's Network and other systems must be deactivated immediately and the departing Covered Person's remote electronic access to personal information must be disabled immediately.

Terminated or resigned Covered Persons shall, before departure, return all files and records in any form containing Personal Information including all information stored on laptops, portable devices (such as thumb/USB/flash drives, CDs, DVDs, cell phones and PDAs), or any other type of media, or in files, records notes or papers.

C. Storage

When not in use, paper documents and files shall be stored in a locked or otherwise secure area such as locked file cabinets, a locked desk or a locked office.

All Covered Persons are prohibited from keeping open files containing Personal Information on their desks when they are not at their desk. At the end of the work day, all files and other records containing Personal Information must be secured to prevent unauthorized disclosure.

D. Electronic Storage

Personal information may not be stored on removable media or portable devices except when there is a critical business need to do so, and shall be encrypted, or password-protected. Portable devices include CD's, DVD's, portable hard drives, portable flash (thumb/USB) drives, laptops, and mobile devices such as smart phones and tablets.

Backup tapes and other local network storage shall be kept secure.

Personal information may not be stored on local hard drives or desktops of VLP computers except as needed in the event of a network outage. Upon the restoration of network services, any Personal Information stored on a local hard drive shall be immediately transferred back to the network and deleted from the local hard drive. Additionally, Personal Information or

confidential data must not be stored on cloud-based storage solutions that are not part of VLP's Network or have not been approved by the WISP Managers.

E. Transmission, Transporting, Remote Access

Sending or removing hard-copy or electronic information contained on portable devices (such as notebook computers, handheld devices, flash/US or external drives) containing Personal Information from the VL P's premises must be done with reasonable precautions to ensure that such information is secure and to prevent unauthorized disclosure.

Transmitting Personal Information from VLP's premises or VLP's Network to any other location electronically for long-term or short-term storage or use is prohibited. This prohibition includes transmission by email attachment or to cloud-based storage that is not part of VLP's Network or has not been approved by the WISP Managers.

It is permissible however, for VLP employees to remotely access Personal Information on VLP's Network provided that they comply with the security procedures described in this policy and that they do not use these methods to accomplish the transfer of Personal Information to another location.

In addition, Personal Information shall not be discussed in public places where conversations can be overheard or recorded, nor shall they be had with individuals who do not have a need to know.

Only those physical documents/files which are necessary to accomplish legitimate business requirements shall be removed from VLP's premises.

When in the course of business Covered Persons are required to send Personal Information about clients to volunteer attorneys, government agencies and others, care must be taken to protect this information and ensure it arrives to its destination uncompromised. Personal information may not be sent via email or internet unless encrypted, which can be done in VLP email by typing "SECURED" in the subject before sending.

F. Disposal

When hard-copy material containing Personal Information is to be disposed of, it shall be redacted, burned, pulverized or shredded so that Personal Information cannot practicably be read or reconstructed. Electronic Personal Information that is no longer needed must be either erased or destroyed so that Personal Information cannot practicably be read or reconstructed.

VI. Remote Access

Remote access to VLP's Network is limited to current VLP employees, interns and students working under the supervision of a VL P employee, and service providers explicitly authorized by VL P to have access. Pro bono attorneys will be given limited access only to their own open cases in LegalServer. Covered Persons who access VLP's Network remotely are responsible for protecting VLP's Personal Information while working remotely. Remote access to VLP's system may only be used to conduct legitimate VLP business and not for personal use.

Data can be more easily intercepted from wireless networks. Covered persons shall not connect to the VLP network through Wi-Fi unless there is no alternative. Under no circumstances shall covered persons access the VL P Network through public or unsecured Wi-Fi. Personal laptops and mobile devices used by covered persons to access the VL P Network shall require passwords or passcodes in order to log in to the device.

VII. Visitors to VLP

Visitors to VLP shall check in at the reception desk. Visitors shall be blocked from accessing any sources (electronic or hard-copy) containing Personal Information except as authorized by the WISP Managers or necessary for business reasons. Volunteer attorneys and other authorized persons assisting clients shall have access only to the Personal Information necessary for their client's representation.

Visitors to VLP who need work space shall be assigned such space only after a VLP employee has taken reasonable precautions to ensure that there are no papers or other documents containing Personal Information visible in the work area to be assigned.

Visitors needing computer access may be provided passwords which permit access to the Internet, and specific programs as necessary (e.g. bankruptcy software) but do not allow the user to access the VLP data servers. Visitors shall not be allowed to use a computer that is logged into the VLP Network unless accompanied by a VLP employee at all times.

VIII. Computer Systems

A. Password Policies

Access to the V LP Network shall be granted only to V L P employees, students and interns working under the supervision of VLP employees, and service providers (where necessary) and only by means of password protected login accounts issued by the VLP or its IT service provider, by way of authorization from one of the WISP Managers. Pro bono attorneys may have restricted access only to necessary client files in VLP's case management system.

After multiple unsuccessful attempts to gain access to VLP's data, systems and/or network the user ID used in the attempts will be locked to prevent further attempts to gain access.

Passwords shall meet industry standard complexity requirements. Covered Persons shall be required to change their passwords regularly.

Access to electronic records containing Personal Information shall be restricted to those individuals that require said information to perform their job duties.

When a user has logged into VLP's Network remotely and has been inactive for the maximum allowable number of minutes of system inactivity, the electronic system shall log the user off the system.

VLP shall promptly prohibit access to all electronic data by Covered Persons who are no longer authorized to have access.

VLP users must take care to guard their network, case management and email passwords. The disclosure of passwords to another person who is not a current VLP employee, supervised student or intern, or authorized service provider is prohibited. The posting of passwords on post- it notes, bulletin boards or elsewhere is prohibited.

B. Locking screen savers

All VLP computers will be equipped with screen savers that lock the computer after an idle period. The screen saver shall require a password to unlock the computer. Users are not permitted to disable the screen saver protection.

C. Network Security Maintenance and Monitoring

VLP shall, directly or through the services of a competent IT service provider, monitor all computer systems for unauthorized use of or access to records and files containing Personal Information.

VLP shall maintain and install on all systems processing or storing Personal Information up-to-date firewall protection, operating system security patches, antivirus and malware protection software reasonably designed to maintain the integrity of the personal information.

IX. Third Party Service Providers

Before engaging with a third-party service provider, VLP shall conduct reasonable due diligence to ensure that any third-party service provider with which VLP shares any Personal Information is capable of protecting Personal Information to the same degree of protection that VLP is required to maintain. VLP shall execute non-disclosure agreements with all third-party service providers that have access to Personal Information.

X. Information Retention

VLP shall collect and maintain Personal Information for as long as reasonably necessary to carry out the purpose of the business, or as otherwise necessary for VLP to comply with local, state or federal regulations or requirements.

XI. Security Awareness Training and Notice

Following the adoption of this WISP, the WISP Managers in conjunction with the Executive Director shall provide training to all Covered Persons within 30 days, or as soon as practicable on the proper use of the computer security system and the importance of personal information security.

Refresher trainings will be presented annually to VLP staff on or before February 28 of each year.

The WISP will be given to all current VLP employees and provided to each new Covered Person. Volunteer attorneys who are given access to their cases on LegalServer shall be given a copy of the WISP at the time they are given their LegalServer account password. Any

amendments to this WISP or new procedures adopted shall be promptly communicated to all staff.

XII. Reviews/Audits All security measures shall be reviewed at least quarterly (on or before March 31, June 30, September 30, and December 31 of each year) by the WISP Managers, Legal Director, Deputy Director, and Executive Director, or whenever a material change occurs in VLP's business practices that may reasonable implicate the security or integrity of records or files containing Personal Information.

The WISP Managers shall be responsible for this review and shall fully apprise VLP management of the results of the review and any recommendations for improved security arising from that review.

XIII. Breach of Security

A. Notification

Any incident involving a breach or potential breach of security, including, but not limited to, all inappropriate requests for sensitive information and other suspicious activity, should be reported to the WISP Managers or Executive Director. The Executive Director should report immediately after being informed of a breach to the Attorney General's Office and the Office of Consumer Affairs & Business Regulation.

B. Incident Review and Reporting

Whenever there is an incident that requires notification under M.G.L. c. 93H, Section 3, there shall be an immediate, fully documented post-incident review, conducted by the WISP Managers and/or VLP's Managers of the events and actions taken, if any, to determine whether any changes in VLP's security practices are required to improve security. Depending on applicable state and federal laws, the incident may need to be reported to the affected persons as well as any other state and/or federal regulators.

C. Policy Violation

Any Covered Persons who violate this policy, in any way, may be subject to disciplinary action, including termination.

For minor infractions, with the definition of "minor" to be determined by the WISP Managers based upon the nature of the violation and the nature of the Personal Information affected by the violation, the Cover Person shall be disciplined by either a verbal or a written warning.

For major infractions, with the definition of "major" to be determined by the WISP Managers based upon the nature of the violation and the nature of the Personal Information affected by the violation, the Covered Person shall be disciplined by suspension or termination. The definition of "major" may include a pattern of three or more "minor" violations.

In addition, Covered Persons may be subject to administrative actions, criminal prosecution and/or civil actions for violations.

XIV. Amendments

This WISP may be amended from time to time. The current policy will be maintained on the VLP shared network drive or SharePoint.

Definitions: **Breach of security** - 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 personal information, 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 personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Covered Person(s) – any fulltime, part time or temporary employee, student intern, volunteer, independent contractor, consultant or other worker.

Credentials – a combination of User ID and password.

Electronic - relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Employee fulltime, part time or temporary employee, volunteer or student intern.

Encryption - the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses - receives stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person - 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, or any of its branches, or any political subdivision thereof.

Personal information - a Massachusetts resident'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 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; 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.

Record or Records - any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Removable Media - In computer storage, removable media refers to storage media which is designed to be removed from the computer without powering the computer off. This includes but is not limited to CDs, DVDs, USB drives, "thumb" drives, flash drives, iPods, and MP3 players.

Service provider - any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

VLP Network – refers to all applications included in VLP's Office 365 subscription, and VLP's case management system, LegalServer.

APPENDIX B

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Section:

17.01 **Purpose and Scope**

(1) Purpose

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope

The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: **Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, 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 personal information, 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 personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical,

electromagnetic or similar capabilities.
Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses, receives stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, 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, or any of its branches, or any political subdivision thereof.

Personal information, a Massachusetts resident'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 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; 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.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

17.03: **Duty to Protect and Standards for Protecting Personal Information**

1. Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal

APPENDIX B

regulations by which the person who owns or licenses such information may be regulated.

2. Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more employees to maintain the comprehensive information security program;

(b) Identifying and assessing reasonably foreseeable internal and 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, including but not limited to:

i. ongoing employee (including temporary and contract employee) training;
ii. employee compliance with policies and procedures; and
iii. means for detecting and preventing security system failures.

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

i. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and

ii. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, which, at a minimum, and to the extent technically feasible, shall have the following elements:

1. Secure user authentication protocols including:

(a) control of user IDs and other identifiers;
(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
(c) 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;
(d) restricting access to active users and active user accounts only; and
(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

2. Secure access control measures that:

(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
(b) 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;

3. 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.
4. Reasonable monitoring of systems, for unauthorized use of or access to personal information;
5. Encryption of all personal information stored on laptops or other portable devices;
6. 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.
7. Reasonably up-to-date versions of system security agent software which must include 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.
8. Education and training of employees on the proper use of the computer security system and

the importance of personal information security.

17.05: **Compliance Deadline**

Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00. This Written Information Security Program was implemented March 1, 2010. Revisions: January 2018. VLP will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.

Volunteer Lawyers Project of the Boston Bar Association

ACKNOWLEDGEMENT AND CERTIFICATION

(Employees and Board Members)

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

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

I acknowledge that failure on my part to practice due care and due diligence with respect to Personal Information and the Organization'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