Written Information Security Program (WISP)

MELISSA J. KRASNOW, VLP LAW GROUP LLP,
WITH PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

A model Written Information Security Program (WISP) addressing the requirements of Massachusetts's Data Security Regulation and the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule. This Standard Document provides general guidance for developing a WISP as may be required by other state and federal laws and best practices. This Standard Document also includes integrated notes with important explanations and drafting tips.

DRAFTING NOTE: READ THIS BEFORE USING DOCUMENT

A Written Information Security Program (WISP) documents the measures that a business, or organization, takes to protect the security, confidentiality, integrity, and availability of the personal information and other sensitive information it collects, creates, uses, and maintains.

This model WISP:

- Addresses the requirements of Massachusetts's Data Security Regulation (Mass. Regs. Code tit. 201, §§ 17.01-17.05) and the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (16 C.F.R. Part 314).
- Provides general guidance for developing a WISP as may be required by other state and federal laws and best practices.

BUSINESS CONSIDERATIONS

While this Standard Document serves as a helpful starting point for drafting any WISP, no model WISP is appropriate for all businesses. In developing a WISP, an organization should consider:

- The size, scope, and type of its business or other activities.
- Its information collection and use practices, including the amount and types of personal and other sensitive information it maintains.
- The need to secure both customer and employee personal information.
- Specific applicable legal requirements, which may depend on, among other things:
  - the nature and industry of the business or organization;
  - the type of information collected and maintained; and
  - the geographic footprint of the business, including the states where the organization's customers and employees reside.

- The resources available to implement and maintain an information security program.

Even when not explicitly required by law, a well-developed and maintained WISP may provide benefits, including:

- Prompting the business to proactively assess risk and implement measures to protect personal and other sensitive information.
- Educating employees and other stakeholders about the actions they need to take to protect personal and other sensitive information.
- Helping to communicate data security expectations and practices to leadership, customers, and other interested parties, such as regulators.
- Establishing that the organization takes reasonable steps to protect personal and other sensitive information, especially in the event of a security incident where litigation or enforcement action could occur.

LEGAL CONSIDERATIONS

This model WISP is helpful in complying with the information security program requirements found in:

- Massachusetts's Data Security Regulation (Mass. Regs. Code tit. 201, §§ 17.01-17.05) (see Massachusetts Data Security Regulation).
- The GLBA Safeguards Rule (16 C.F.R. Part 314) (see Gramm-Leach-Bliley Act Safeguards Rule).
- Oregon's Identity Theft Protection Act (Or. Rev. Stat. § 646A.622) (see Oregon Identity Theft Protection Act).
- Other state laws and best practices with data security requirements (see Other State Data Security Safeguards Laws and Best Practices and Resources).

Massachusetts Data Security Regulation

The Massachusetts Data Security Regulation (Mass. Regs. Code tit. 201, §§ 17.01-17.05) provides the most detailed WISP requirements, and applies to any business that collects Massachusetts residents' personal information, no matter where the business is located. This Standard Document follows the Massachusetts Data Security Regulation's requirements, and should be used together with Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation (7-523-1520).

Gramm-Leach-Bliley Act Safeguards Rule

The GLBA applies to financial institutions that collect consumers' non-public personal information (NPI). The GLBA Safeguards Rule requires companies to develop, implement, and maintain a WISP that includes appropriate administrative, technical, and physical safeguards to protect consumer information (16 C.F.R. § 314.3). It also requires them to contractually obligate their service providers who handle NPI to implement and maintain similar safeguards (16 C.F.R. § 314.4).

The Safeguards Rule defines WISP requirements more broadly than the Massachusetts Data Security Regulation, so this Standard Document is also suitable to use as a basis for developing a GLBA-compliant WISP, using the alternative language to define personal information as explained in Drafting Note, Scope: Personal Information. See Practice Note, GLBA: The Financial Privacy and Safeguards Rules: The Safeguards Rule (4-578-2212).

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) applies to certain health care entities and their service providers (business associates). The HIPAA Security Rule requires covered entities and their business associates to:

- Implement and maintain specified administrative, technical, and physical safeguards.
- Implement reasonable and appropriate written policies and procedures.
- Maintain a written record of required activities, such as risk assessments.

(See 45 C.F.R. Part 164, Subpart C and Practice Note, HIPAA Security Rule: Safeguards and Related Organizational and Document Requirements (5-502-1269).)

Covered entities and their business associates should:

- Ensure that their information security policies and procedures are HIPAA-compliant.
- Recognize that a WISP may provide them with a convenient way to organize and describe their information security program.
- Develop and maintain a WISP, if required by other applicable laws, such as the Massachusetts Data Security Regulation.

Oregon Identity Theft Protection Act

Like Massachusetts, Oregon has enacted a comprehensive statute that mandates the implementation of safeguards to protect residents' personal information (Or. Rev. Stat. § 646A.622). Oregon requires that organizations develop, implement, and maintain **reasonable** safeguards to protect the security, confidentiality, and integrity of the personal information they use. A business meets the reasonableness standard if it either:

- Complies with the GLBA, HIPAA, or any federal or state law that affords greater protection of personal information than the Oregon statute.
- Implements an information security program that includes specific:
  - administrative safeguards;
  - technical safeguards; and
  - physical safeguards, similar to those required by Massachusetts, all with an emphasis on risk assessment (Or. Rev. Stat. § 646A.622(2)(d)).

Oregon also provides flexibility for small businesses to scale their programs in a manner that is appropriate to their size, complexity, activities, and the sensitivity of the personal information they collect (Or. Rev. Stat. § 646A.622(4)). The same leeway is granted to all organizations covered by the GLBA Safeguards Rule (16 C.F.R. § 314.3(a)), while the HIPAA Security Rule permits a similar "flexibility of approach" for covered entities and their business associates to choose security measures appropriate to their size, complexity, capabilities, and risks (45 C.F.R. § 164.306(b)).

Other State Data Security Safeguards Laws

Several other states have enacted statutes that require organizations to protect personal information by developing, implementing, and maintaining reasonable information security safeguards. These proactive data protection laws are in addition to the data breach notification statutes enacted by all but a few states. See Data Breach Notification Laws: State Q&A Tool (3-578-0925).

Some other state laws require that organizations implement reasonable and appropriate security measures to protect personal information even if they do not specifically mandate a WISP.

For example, businesses that own, license, or maintain California residents' personal information must:

- Implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure.
- Contractually require any nonaffiliated third party to whom they disclose personal information to implement and maintain reasonable security measures.
- Implement specific measures to protect personal information when disposing of it.

(Cal. Civ. Code §§ 1798.81, 1798.81.5.)

Similarly, Texas law requires that businesses protect what the law deems to be sensitive personal information by:

- Implementing and maintaining reasonable data protection procedures, including taking any appropriate corrective actions.
- Securely destroying personal information or rendering it unreadable or indecipherable when it is no longer to be retained.

(Tex. Bus. & Com. Code Ann. § 521.052.)

The Rhode Island Identity Theft Protection Act of 2015 requires businesses to:

- Implement and maintain a risk-based information security program with reasonable security procedures and practices that protect personal information and are appropriate to:
  - the organization's size and scope;
  - the nature of the personal information; and

  - the purpose for which the personal information was collected.
- Retain personal information no longer than is reasonably required:
  - to provide requested services;
  - to meet the purposes for which the personal information was collected;
  - in accordance with a written retention policy; or
  - by law.
- Use secure methods to destroy personal information.
- Contractually require any nonaffiliated third party to whom they disclose personal information to implement and maintain similar reasonable security procedures and practices.

(R.I. Gen. Laws § 11-49.3-2.)

As amended on January 1, 2017, Illinois's Personal Information Protection Act:

- Calls for organizations to implement and maintain reasonable security measures.
- Deems entities that comply with other federal or state laws, such as GLBA or those that offer greater personal information protection, to be in compliance.

(815 Ill. Comp. Stat. Ann. 530/1.)

Best Practices and Resources

Several state and federal agencies have issued guidance documents to assist large and small businesses and other organizations in performing risk assessments and developing, implementing, and maintaining their information security programs, including:

- The Federal Trade Commission's (FTC):
  - Protecting Personal Information: A Guide for Business, which provides a five-principle approach to building an information security plan; and
  - Start with Security: A Guide for Business, which offers ten lessons learned from its data security enforcement actions, with practical guidance on how to reduce risks for all businesses.
- The National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework), which organizes various globally-recognized industry standards and best practices into a model that any organization can adapt and use to identify risks and build an information security program (see Practice Note, The NIST Cybersecurity Framework (5-599-6825)).
- The California Attorney General's Cybersecurity in the Golden State, which includes practical recommendations for managing information security risks focused on small to medium-sized businesses.

These resources' recommendations are comparable to the Massachusetts Data Security Regulation's requirements and other similar state and federal laws, while providing additional technical guidance in an accessible form.

DRAFTING AND IMPLEMENTATION CONSIDERATIONS

An organization's WISP should be consistent with its current data collection and information security practices, unless specific program plan documentation is in place to close any gaps. Businesses create potential compliance, enforcement, and litigation risks by putting in place and committing to WISPs they do not follow.

Therefore, before developing a WISP, an organization should:

- Gather all relevant information regarding the personal and other sensitive information that it collects, creates, uses, and maintains, including current information security practices.
- Identify all applicable laws and standards that affect the organization's use of personal or other sensitive information, including any contractual obligations.
- Define the WISP's scope, including the personal information, any other sensitive information, and legal requirements it intends to address.

(See Drafting Note, Scope and Practice Note, Written Information Security

Programs: Compliance with the Massachusetts Data Security Regulation: Preliminary Considerations (7-523-1520).)

Related Policies and Other Documents

While an organization's WISP outlines the purpose, scope, and core elements of its information security program, specific security measures are often defined in related documents, including:

- Risk assessment reports and remediation plans.
- One or more workforce-facing information security policy documents, such as those that that establish policies regarding:
  - information classification and handling practices;
  - user access management and passwords;
  - computer and network security;
  - physical security;
  - incident reporting and response;
  - employee and contractor use of technology, for example, Acceptable Use and Bring Your Own Device to Work (BYOD) policies (see Standard Documents, IT Resources and Communications Systems Policy (8-500-5003) and Bring Your Own Device to Work (BYOD) Policy (1-521-3920)); and
  - information systems acquisition, development, and maintenance.
- Process and procedures documents that detail how to implement and maintain particular safeguards, typically for use by technical or other support staff.

Awareness and Training

Organizations should also consider how to best distribute and build awareness of the WISP and related policies, processes, and procedures. For example, businesses may choose to integrate information security training with existing ethics and compliance programs.

At a minimum, the organization should:

- Specifically train all employees and contractors, especially those who handle personal and other sensitive information as part of their duties, on the WISP and relevant policies and procedures.
- Require all employees and contractors to formally acknowledge their receipt and understanding of the documentation and training, using written forms or an online learning system.
- Retain training and acknowledgment records.

ASSUMPTIONS

This written information security program (WISP) assumes that:

- **The organization only collects, creates, uses, and maintains US residents' personal information.** If the organization handles personal information in non-US locations or plans to transfer personal information to the US, it may be subject to data security or privacy laws in those other jurisdictions. Privacy laws vary significantly, and are often more stringent outside the US, especially in the EU (see Data protection: Country Q&A Tool (2-502-1510) to compare laws in the US and selected non-US locations).

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

The objectives of this comprehensive written information security program ("WISP") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards [COMPANY] has selected to protect the personal information it collects, creates, uses, and maintains. This WISP has been developed in accordance with the requirements of the Massachusetts Data Security Regulation, Mass. Regs. Code tit. 201, §§ 17.01-17.05, other similar US state laws, and [LIST ADDITIONAL APPLICABLE LAWS AND OBLIGATIONS].

In the event of a conflict between this WISP and any legal obligation or other [COMPANY] policy or procedure, the provisions of this WISP shall govern, unless the Information Security Coordinator specifically reviews, approves, and documents an exception (see Section 3).

DRAFTING NOTE: WISP OBJECTIVES: APPLICABLE LAWS AND OBLIGATIONS

In this section, the organization should identify all applicable laws, standards, policies, and contractual obligations that may affect its use of personal information or impose obligations on its information security program and as will be addressed by the WISP (see Drafting Notes, Legal Considerations and Drafting and Implementation Considerations).

1. Purpose. The purpose of this WISP is to:

(a) Ensure the security, confidentiality, integrity, and availability of personal [and other sensitive] information [COMPANY] collects, creates, uses, and maintains;

(b) Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information;

(c) Protect against unauthorized access to or use of [COMPANY]-maintained personal [and other sensitive] information that could result in substantial harm or inconvenience to any customer or employee; and

(d) Define an information security program that is appropriate to [COMPANY]'s size, scope, and business; its available resources; and the amount of personal [and other sensitive] information that [COMPANY] owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

DRAFTING NOTE: PURPOSE

This purpose statement tracks the high-level WISP requirements stated in the Massachusetts Data Security Regulation and other similar state and federal laws, including the GLBA (see Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Massachusetts Regulation: General WISP Requirements (7-523-1520)).

2. Scope. This WISP applies to [all employees, contractors, officers, and directors of [COMPANY]/[DEFINE SCOPE]]. It applies to any records that contain personal [and other sensitive] information in any format and on any media, whether in electronic or paper form.

(a) For purposes of this WISP, "personal information" means either a US resident's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:

(i) Social Security number;

(ii) Driver's license number, other government-issued identification number, including passport number, or tribal identification number;

(iii) 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 the individual's financial account [GLBA:, and any personally identifiable financial information or consumer list, description, or other grouping derived from personally identifiable financial information, where personally identifiable financial information includes any information:

(A) A consumer provides [COMPANY] to obtain a financial product or service;

(B) About a consumer resulting from any transaction involving a financial product or service with [COMPANY]; or

(C) Information [COMPANY] otherwise obtains about a consumer in connection with providing a financial product or service];

(iv) [Health information, including information [regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional/created or received by [COMPANY]]/[HIPAA: which identifies or for which there is a reasonable basis to believe the information can be used to identify the individual and which relates to the past, present, or future physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual]];

(v) Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer;

(vi) Biometric data collected from the individual and used to authenticate the individual during a transaction, such as an image of a fingerprint, retina, or iris; or

(vii) Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

(b) Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, state, or local government records. [

(c) For purposes of this WISP, "sensitive information" means data that:

(i) [COMPANY] considers to be highly confidential information; or

(ii) If accessed by or disclosed to unauthorized parties, could cause significant or material harm to [COMPANY], its customers, or its business partners.

(iii) Sensitive information includes, but is not limited to, personal information. [See [COMPANY]'s information classification policy, available at [REFERENCE TO POLICY].]]

DRAFTING NOTE: SCOPE

The organization should determine whether the WISP applies enterprise-wide or only to selected business units or activities and adjust the scope statement as needed (see Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Scope of the WISP (7-523-1520)).

PERSONAL INFORMATION

The definition of personal information provided follows the generally-applicable Massachusetts Data Security Regulation and similar state laws, including those of Oregon and Rhode Island (Or. Rev. Stat. § 646A.602(11); R.I. Gen. Laws § 11-49.3-3). While there are similarities, each state's statute defines personal information differently, so this definition combines the elements in the Massachusetts, Oregon, and Rhode Island laws.

Generally, the WISP should define personal information considering:

- The data the business collects, creates, uses, or maintains.
- The organization's near-term business plans, such as the states where its customers or employees may reside.
- Applicable laws (see Drafting Note, Legal Considerations) to protect data that the

organization references in its privacy policy or other public statements.

- What is otherwise considered personal information by the organization, including any information that it must protect by contract with third parties.

If applicable:

- Section 2(a)(iii) should include the additional text to meet GLBA's definition of non-public personal information (see 16 C.F.R. § 313.3(n)(1)).
- Section 2(a)(iv) should use the optional text regarding HIPAA to meet HIPAA's requirements (see 45 C.F.R. § 160.103).

SENSITIVE INFORMATION

If the WISP is intended to cover other data that the organization considers to be sensitive, in addition to personal information, then the optional text should be included in this section and throughout the WISP. For example, a business may wish to apply the same WISP to highly confidential information regarding its products, business plans, or certain operations (or may be required to do so by contract with third parties).

Sensitive or highly confidential information:

- Typically includes data that if accessed by or disclosed to unauthorized parties could cause **significant or material harm** to the organization, its customers, or its business partners.
- Includes, but is not limited to, personal information.
- May be contrasted to an organization's less sensitive, but still non-public internal use only or confidential information.

If the organization has an information classification policy, for example, as part of its information security policies and procedures (see Section 5), the WISP should include a reference as shown in the optional text.

3. Information Security Coordinator. [COMPANY] has designated [TITLE] to implement, coordinate, and maintain this WISP (the "Information Security Coordinator"). The Information Security Coordinator shall be responsible for:

(a) Initial implementation of this WISP, including:

(i) Assessing internal and external risks to personal [and other sensitive] information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);

(ii) Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 5);

(iii) Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal [and other sensitive] information (see Section 6);

(iv) Ensuring that the safeguards are implemented and maintained to protect personal [and other sensitive] information throughout [COMPANY], where applicable (see Section 6);

(v) Overseeing service providers that access or maintain personal [and other sensitive] information on behalf of [COMPANY] (see Section 7);

(vi) Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 8);

(vii) Defining and managing incident response procedures (see Section 9); and

(viii) Establishing and managing enforcement policies and procedures for this WISP, in collaboration with [COMPANY] human resources and management (see Section 10).

(b) Employee, contractor, and (as applicable) stakeholder training, including:

(i) Providing periodic training regarding this WISP, [COMPANY]'s safeguards, and relevant information security policies and procedures for all employees, contractors, and (as applicable) stakeholders who have or may have access to personal [or other sensitive] information;

(ii) Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through [written acknowledgement forms/[DESCRIBE ANY ONLINE ACKNOWLEDGMENT PROCESS]]; and

(iii) Retaining training and acknowledgment records.

(c) Reviewing the WISP and the security measures defined herein at least annually, or whenever there is a material change in [COMPANY]'s business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information (see Section 11).

(d) Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or [COMPANY]'s information security policies and procedures.

(e) Periodically reporting to [COMPANY] management regarding the status of the information security program and [COMPANY]'s safeguards to protect personal [and other sensitive] information.

DRAFTING NOTE: INFORMATION SECURITY COORDINATOR

Considerations for designating an information security coordinator depend on the organization's specific circumstances and may include:

- The organization's size, industry, and regulators.
- The types of personal and other sensitive information the organization owns or maintains on behalf of others.
- The employees responsible for the organization's compliance with security requirements, including compliance with its internal policies and procedures, contracts, and relevant laws and industry standards.
- Leadership support and sponsorship to ensure the information security coordinator has sufficient authority to implement and enforce the WISP.

The organization should also consider the appropriate business units to involve in program oversight, which may include:

- Legal.
- Information technology (IT).
- Privacy or a broader ethics and compliance unit.

The specific title used for the information security coordinator role may also vary according to the organization's size, industry, and other characteristics. The WISP should be drafted to refer to the coordinator by current title, and not individual name, to minimize maintenance requirements and any potential confusion if personnel change.

4. Risk Assessment. As a part of developing and implementing this WISP, [COMPANY] will conduct a periodic, documented risk assessment[, at least annually, or whenever there is a material change in [COMPANY]'s business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information].

(a) The risk assessment shall:

(i) Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal [or other sensitive] information.

(ii) Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal [and other sensitive] information.

(iii) Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

(A) Employee, contractor, and (as applicable) stakeholder training and management;

(B) Employee, contractor, and (as applicable) stakeholder compliance with this WISP and related policies and procedures;

(C) Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and

(D) [COMPANY]'s ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

(b) Following each risk assessment, [COMPANY] will:

(i) Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks.

(ii) Reasonably and appropriately address any identified gaps.

(iii) Regularly monitor the effectiveness of [COMPANY]'s safeguards, as specified in this WISP (see Section 8).

DRAFTING NOTE: RISK ASSESSMENT

Risk assessment is a critical element of any information security program. Information security risks are best understood using this simple equation: **risk = threat + vulnerability**.

Threats may include external bad actors or internal (employee or contractor) lapses, whether inadvertent or intentional. Vulnerabilities cover a wide range of issues related to process, people, and technology, such as:

- Untrained or inattentive individuals.
- Improperly secured facilities.
- Poor implementation, configuration, or maintenance practices.
- Flaws in network and computer assets, including hardware, software, and application issues.

See Drafting Note, Best Practices and Resources and Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Identifying and Minimizing Reasonably Foreseeable Internal and External Risks (7-523-1520) for guidance on risk assessments.

Risks change over time as:

- Novel threats emerge.
- Vulnerabilities are identified and become widely-known.
- The business evolves, especially when it:
  - makes changes in data collection and handling practices;
  - introduces new or materially changed products and services;
  - alters its business processes and practices; or
  - deploys new, or updates existing, network and computer environments.

Organizations should develop processes to assess risks on an ongoing basis and periodically update their formal risk assessment. These updates should be made at least annually or whenever there is a material change in applicable business practices.

5. Information Security Policies and Procedures. As part of this WISP, [COMPANY] will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and (as applicable) other stakeholders to:

(a) Establish policies regarding:

(i) Information classification;

(ii) Information handling practices for personal [and other sensitive] information, including the storage, access, disposal, and external transfer or transportation of personal [and other sensitive] information;

(iii) User access management, including identification and authentication (using passwords or other appropriate means);

(iv) Encryption;

(v) Computer and network security;

(vi) Physical security;

(vii) Incident reporting and response;

(viii) Employee and contractor use of technology, including Acceptable Use and Bring Your Own Device to Work (BYOD); and

(ix) Information systems acquisition, development, operations, and maintenance.

(b) Detail the implementation and maintenance of [COMPANY]'s administrative, technical, and physical safeguards (see Section 6).

DRAFTING NOTE: INFORMATION SECURITY POLICIES AND PROCEDURES

Information security policies:

- Serve as a foundational administrative safeguard by providing clear guidance and limits for employees, contractors, and other stakeholders.
- Explain how the organization classifies various forms of data, which in turn defines the level and nature of safeguards to be applied.
- Should be written for and accessible to all employees, contractors, and other stakeholders.
- Should be periodically reviewed and updated as risks and the business change.

Information security procedures:

- Document how the organization implements and maintains its selected safeguards.
- Often include technical details intended primarily for IT or other support staff.

6. Safeguards. [COMPANY] will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal [or other sensitive] information that [COMPANY] owns or maintains on behalf of others.

(a) Safeguards shall be appropriate to [COMPANY]'s size, scope, and business; its available resources; and the amount of personal [and other sensitive] information that [COMPANY] owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

(b) [COMPANY] shall document its administrative, technical, and physical safeguards in [COMPANY]'s information security policies and procedures (see Section 5).

(c) [COMPANY]'s administrative safeguards shall include, at a minimum:

(i) Designating one or more employees to coordinate the information security program (see Section 3);

(ii) Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 4);

(iii) Training employees in security program practices and procedures, with management oversight (see Section 3);

(iv) Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7); and

(v) Adjusting the information security program in light of business changes or new circumstances (see Section 11);

(d) [COMPANY]'s technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:

(i) Secure user authentication protocols, including:

(A) Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;

(B) Restricting access to active users and active user accounts only, including preventing terminated employees or contractors from accessing systems or records; and

(C) Blocking access to a particular user identifier after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

(ii) Secure access control measures, including:

(A) Restricting access to records and files containing personal [or other sensitive] information to those with a need to know to perform their duties; and

(B) Assigning unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) to each individual with computer or network access that are reasonably designed to maintain security.

(iii) Encryption of all personal [or other sensitive] information traveling wirelessly or across public networks.

(iv) Encryption of all personal [or other sensitive] information stored on laptops or other portable or mobile devices [, and to the extent technically feasible, personal [or other sensitive] information stored on any other device or media (data-at-rest)].

(v) Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal [or other sensitive] information or other attacks or system failures.

(vi) Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal [or other sensitive] information.

(vii) Reasonably current system security software (or a version that can still be supported with reasonably current patches and malware definitions) that (1) includes malicious software ("malware") protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

(e) [Company]'s physical safeguards shall, at a minimum, provide for:

(i) Defining and implementing reasonable physical security measures to protect areas where personal [or other sensitive] information may be accessed, including reasonably restricting physical access and storing records containing personal [or other sensitive] information in locked facilities, areas, or containers.

(ii) Preventing, detecting, and responding to intrusions or unauthorized access to personal [or other sensitive] information, including during or after data collection, transportation, or disposal.

(iii) Secure disposal or destruction of personal [or other sensitive] information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

DRAFTING NOTE: SAFEGUARDS

The safeguards detailed here track the Massachusetts Data Security Regulation and other similar state laws, including Oregon's statute, as well as the GLBA Safeguards Rule. Organizations that are subject to HIPAA should update the administrative, technical, and physical safeguards accordingly.

Organizations should not only examine applicable laws but also determine the feasibility of implementing and maintaining safeguards in their environments. According to guidance from the Massachusetts Office of Consumer Affairs and Business Regulation, "technically feasible" means that if there is a reasonable means through technology to accomplish a required result, the organization must use such reasonable means.

Legal requirements generally call for encrypting personal information when it is stored on mobile devices or transmitted wirelessly or over public networks. However, to better manage risk, organizations may choose to expand their encryption programs to include any stored personal information (data-at-rest) to the extent feasible, as shown in the optional text. For example, many federal and state data breach notification laws provide safe harbor from notice requirements when encryption is used (and encryption keys or other controls are not compromised by a breach).

To minimize potential compliance risk and liability, a business should meet the safeguards commitments it makes in its WISP or have a reasonable remediation plan in place and documented to close any gaps.

7. Service Provider Oversight. [COMPANY] will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain personal [or other sensitive] information on its behalf by:

(a) Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and [COMPANY]'s obligations.

(b) Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and [COMPANY]'s obligations.

(c) Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws and [COMPANY]'s obligations.

DRAFTING NOTE: SERVICE PROVIDER OVERSIGHT

Organizations should:

- Conduct data security due diligence on their service providers before engagement and monitor and audit ongoing performance.
- Identify their applicable existing service providers and, if necessary, amend their contracts to ensure compliance with applicable laws and the WISP.
- Include specific requirements in new service provider agreements involving personal or other sensitive information to address compliance with applicable laws and the WISP.
- Address service provider oversight in employee training.

See Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Third-Party Service Providers (7-523-1520).

8. Monitoring. [COMPANY] will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal [or other sensitive] information. [COMPANY] shall reasonably and appropriately address any identified gaps.

9. Incident Response. [COMPANY] will establish and maintain policies and procedures regarding information security incident response (see Section 5). Such procedures shall include:

(a) Documenting the response to any security incident or event that involves a breach of security;

(b) Performing a post-incident review of events and actions taken; and

(c) Reasonably and appropriately addressing any identified gaps.

10. Enforcement. Violations of this WISP will result in disciplinary action, in accordance with [COMPANY]'s information security policies and procedures and human resources policies. Please see [REFERENCE TO HR POLICIES] for details regarding [COMPANY]'s disciplinary process.

DRAFTING NOTE: ENFORCEMENT

Organizations must impose disciplinary measures for WISP violations under the Massachusetts Data Security Regulation. Other laws may require similar sanctions. To avoid employee confusion and potential conflicts, rather than creating its own disciplinary process, the WISP should refer to established human resources policies and processes. Information security policies and procedures may further define prohibited actions and compliance processes.

11. Program Review. [COMPANY] will review this WISP and the security measures defined herein at least annually, or whenever there is a material change in [COMPANY]'s business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information.

(a) [COMPANY] shall retain documentation regarding any such program review, including any identified gaps and action plans.

DRAFTING NOTE: PROGRAM REVIEW

The Massachusetts Data Security Regulation and best practices require that a business review its WISP on at least an annual basis or whenever there is a material change in business practices that may implicate the security or integrity of records that contain personal or other sensitive information.

12. Effective Date. This WISP is effective as of [DATE].

(a) Revision History: [Original publication/[NOTE SUBSEQUENT REVISIONS]].

DRAFTING NOTE: EFFECTIVE DATE

The WISP should include an effective date and identify any subsequent revisions. The organization should briefly note in the revision history any material updates and their drivers, such as a periodic program review or change in business processes, laws, or identified risks. The organization should retain prior versions of the WISP to demonstrate the program that was in effect at any particular time.