

# WRITTEN INFORMATION SECURITY PROGRAM (WISP)

<<Insert Date>>

Information Security Office  
ENTER BUSINESS NAME HERE

# WRITTEN INFORMATION SECURITY PROGRAM (WISP)

Responsible Office: <<TBD>>

Effective Date: <<Insert Date>>

## TABLE OF CONTENTS

I.	Program Statement.....	2
II.	Objective .....	2
III.	Scope .....	2
IV.	Applicability .....	3
V.	Information Security Coordinator .....	3
VI.	Regulatory Compliance Policies, Standards .....	4
VII.	Waivers and Exceptions .....	4
VIII.	Enforcement and Disciplinary Action.....	5
IX.	Breach of Data Security Protocol .....	5
	Appendix A .....	6
	The State of Connecticut, Substitute Senate Bill No. 949, Public Act No. 15-142:6	
	The Commonwealth of Massachusetts 201 CMR 17.00:.....	6
	HIPAA PHI: Definition of PHI and the List of 18 Identifiers: .....	6

## Revision History

Date of Change	Responsible	Summary of Change
September 2018	TTG SAS	TTG template revision v4

## WRITTEN INFORMATION SECURITY PROGRAM (WISP)

Responsible Office: <<TBD>>

Effective Date: <<Insert Date>>

### I. PROGRAM STATEMENT

**enter Business name here** ("the Company") recognizes that in certain instances it must collect, store and use Social Security Numbers, drivers' license numbers, financial account numbers, health status and other sensitive, confidential or personal information relating to its customers, employees and individuals associated with the Company. The Company is dedicated to collecting, handling, storing and using that Information properly and securely.

**For HIPAA Compliance ONLY:** For purposes of this written information security program ("WISP") this Information defined as "confidential information" or "personal information" by State of Connecticut and the Commonwealth of Massachusetts statutes together with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule regulating the use and disclosure of Protected Health Information (PHI) will be referred to as "confidential" information. The applicable data elements and regulatory references are provided in **Appendix A**.

### II. OBJECTIVE

The objectives in the development and implementation of this WISP:

- (1) To provide a formal information security program for achieving the collection of policies, standards and operating procedures supporting the confidentiality, integrity and availability of the Company's technology information;
- (2) To use risk-based methodology to provide assurance that controls and expenditures are commensurate with the risks to which the Company is exposed and prioritize management decisions to address the highest risks;
- (3) To create effective administrative, technical and physical safeguards for the protection of Confidential Information maintained by the Company, including sensitive "confidential" information pertaining to the Company's customers, employees and business partners as well as other confidential and sensitive institutional and third party information;
- (4) To comply with our obligations under law for all applicable federal and state law and written policies of the states contained in the agreement.

### III. SCOPE

In formulating and implementing the WISP, the Company has addressed and incorporated the following protocols:

- (1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing "confidential" information;
- (2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the "confidential" information;

## WRITTEN INFORMATION SECURITY PROGRAM (WISP)

Responsible Office: <<TBD>>

Effective Date: <<Insert Date>>

- (3) Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
- (4) Designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of safeguards for protection of "confidential" information as set forth in all applicable federal and state law; and
- (5) Implemented regularly monitoring of the effectiveness of those safeguards.

### IV. APPLICABILITY

This WISP applies to all the Company customers, employees and individuals associated with the Company, whether full-time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the Company, including any Third Party Provider services to the Company, who create, use or otherwise require access or interaction with any Company Information or Company Information Resource on behalf of the Company.

This Program applies to Information defined as "confidential information", including all information collected, stored or used by or on behalf of any operational unit, department and person in connection with Company operations. In the event that any particular information is governed by more specific requirements under other Company policies or procedures, the more specific requirements shall take precedence over this Program to the extent there is any conflict.

### V. INFORMATION SECURITY COORDINATOR

The Company has designated <<TBD>>, <<Position>> to implement, supervise and maintain the WISP. That designated employee (the "Information Security Coordinator" or "ISC") will be responsible for:

- (1) Implementation and periodic oversight of the WISP by reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing "confidential" information.
- (2) Ensuring initial workforce training and conducting an annual training session for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to "confidential" information on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the firm's requirements for ensuring the protection of "confidential" information.
- (3) Regular testing of the WISP's safeguards.
- (4) Evaluating the ability of each of our third party service providers to implement and maintain appropriate security measures for the "confidential" information to which we have permitted them access, consistent with the safeguards for protection of "confidential" information as set forth in all applicable federal and

# WRITTEN INFORMATION SECURITY PROGRAM (WISP)

**Responsible Office:** <<TBD>>

**Effective Date:** <<Insert Date>>

state law; and requiring such third party service providers by contract to implement and maintain appropriate security measures.

## VI. REGULATORY COMPLIANCE POLICIES, STANDARDS

This WISP includes, and incorporates by reference, the Information Security Policy to establish information or cybersecurity security standards and polices. Additional policies or standards are set forth as compliance requirements as follows:

POLICY	PURPOSE
<b>INFORMATION SECURITY POLICY (ISP)</b>	<b>ISP</b> - Defines the technical controls and security configurations users and the Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the protected data.
<b>ACCEPTABLE USE POLICY (AUP)</b>	<b>AUP</b> - How employees use information resources in concert with the Information Security Policy
<b>BUSINESS CONTINUITY PLAN (BCP) AND DISASTER RECOVERY PLAN (DRP)</b>	<b>BCP</b> - How employers and employees stay in touch and keep doing their jobs in the event of a disaster or emergency  <b>DRP</b> - Written processes for how the business recovers technology resources and systems lost in a disaster
<b>INCIDENT RESPONSE POLICY (IRP)</b>	<b>IRP</b> - How data security events are reported and investigated

## VII. WAIVERS AND EXCEPTIONS

Individuals subject to the mandatory requirements or standards set forth in this WISP, or the Information Security Policy, may request that the ISC grant a waiver or exception from a particular requirement or standard that cannot practicably be followed without substantial operational hardship or excessive cost, and the ISC may in his/her discretion grant such waiver or exception provided that:

- (1) the waiver or exception would not result in a violation of applicable law or regulation; and
- (2) that the ISC imposes, wherever possible, other alternative requirements or standards that serve the purposes of the WISP and/or Information Security Policy but are less burdensome on the particular individual or his/her department or unit.

## WRITTEN INFORMATION SECURITY PROGRAM (WISP)

Responsible Office: <<TBD>>

Effective Date: <<Insert Date>>

### VIII. ENFORCEMENT AND DISCIPLINARY ACTION

The Company reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with the WISP. Violations of the WISP will result in appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks, or other employment related discipline up to and including suspension or termination of employment, depending on the circumstances and relevant factors such as the nature and severity of the violation and whether the violation was knowing, intentional or repeated.

### IX. BREACH OF DATA SECURITY PROTOCOL

Should any employee know of a security breach at any of our facilities, or that any unencrypted "confidential" information has been lost or stolen or accessed without authorization, or that encrypted "confidential" information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

- Employees are to notify the ISC or department head in the event of a known or suspected security breach or unauthorized use of "confidential" information.
- The ISC shall be responsible for working with senior management to draft a security breach notification to be provided to the Connecticut Office of the Attorney General and/or the Massachusetts Office of Consumer Affairs and Business Regulation and the Massachusetts Attorney General's office. The security breach notification shall include the following:
  - A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of "confidential" information;
  - The number of Massachusetts residents affected at the time the notification is submitted;
  - The steps already taken relative to the incident;
  - Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
  - Information regarding whether law enforcement officials are engaged in investigating the incident.
- The ISC will follow the Incident Response Policy providing further information on incident response required actions.

## WRITTEN INFORMATION SECURITY PROGRAM (WISP)

Responsible Office: <<TBD>>

Effective Date: <<Insert Date>>

### APPENDIX A

The regulatory definitions for "personal" and "confidential" from the (a) State of Connecticut Substitute Senate Bill No. 949, Public Act No. 15-142; (b) the Commonwealth of Massachusetts 201 CMR 17.00; and (c) the HIPAA Privacy Rule regulating the use and disclosure of PHI are as follows:

#### **The State of Connecticut, Substitute Senate Bill No. 949, Public Act No. 15-142:**

Connecticut's term "Confidential information" means an individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation, personally identifiable information subject to 34 CFR 99, as amended from time to time and protected health information, as defined in 45 CFR 160.103, as amended from time to time. In addition, "confidential information" includes any information that a state contracting agency identifies as confidential to the contractor. "Confidential information" does not include information that may be lawfully obtained from publicly available sources or from federal, state, or local government records that are lawfully made available to the general public.

#### **The Commonwealth of Massachusetts 201 CMR 17.00:**

"Personal Information" means 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.

#### **HIPAA PHI: Definition of PHI and the List of 18 Identifiers:**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information.<sup>1</sup> To fulfill this requirement, HHS published what are commonly known as the HIPAA [Privacy Rule](#) and the HIPAA [Security Rule](#). The Privacy Rule, or *Standards for Privacy of Individually*

## WRITTEN INFORMATION SECURITY PROGRAM (WISP)

**Responsible Office:** <<TBD>>

**Effective Date:** <<Insert Date>>

*Identifiable Health Information*, establishes national standards for the protection of certain health information. The *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI).

**Protected Health Information (PHI)** is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy rule, the Safe Harbor Method of De-Identification requires 18 identifiers be removed as follows:

1. Names;
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census:
  - (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and



## WRITTEN INFORMATION SECURITY PROGRAM (WISP)

**Responsible Office:** <<TBD>>

**Effective Date:** <<Insert Date>>

18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

There are also additional standards and criteria to protect individual's privacy from re-identification. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. For example, a subject's initials cannot be used to code their data because the initials are derived from their name. Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study. In other words, the information would still be considered identifiable if there was a way to identify the individual even though all of the 18 identifiers were removed.