

# WRITTEN INFORMATION SECURITY PROGRAM (WISP)

## SECURITY AWARENESS TRAINING POLICY

<<Legal Entity>> (TEMPLATE – Smaller Entity)

Responsible Office: <<TBD>>

Effective Date: << INSERT DATE >>

### REVISION HISTORY

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

### I. OBJECTIVE:

To establish a security awareness and training policy for all members of Company's workforce, including management.

All workforce members shall receive appropriate training concerning Company's security policies and procedures. Such training shall be provided prior to the effective date of the HIPAA Security Rule and on an ongoing basis to all new employees. Such training shall be repeated annually for all employees.

### II. APPLICABILITY

This security awareness and training policy 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 providing services to the Company, who create, use or otherwise access or interact with any Company Information or Company Information Resource.

This Program applies to all Company 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.

### III. SECURITY AWARENESS POLICY

The Company must implement a security awareness and training program for all owners, managers, employees and independent contractors, including temporary and contract

# WRITTEN INFORMATION SECURITY PROGRAM (WISP)

## SECURITY AWARENESS TRAINING POLICY

### <<Legal Entity>> (TEMPLATE – Smaller Entity)

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

**Effective Date:** << INSERT DATE >>

employees who have access to “confidential” information and individuals associated with the Company.

Employees, business partners and individuals associated with the Company who have access to the Company information systems must understand how to protect the confidentiality, integrity, and availability of information systems.

The Company must develop, implement, and regularly review a formal, documented program for providing security training, education and awareness to its faculty, staff, students, and volunteers. The Company WISP has designated (the “<<Information Security Coordinator>>” or “ISC”) to be responsible for conducting an annual training session.

Company employees and individuals associated with the Company who have access to the Company information systems must be provided with regular training, supporting reference materials, and reminders to enable them to appropriately protect Company information systems. Such training may be provided at the Company facility or via remote training methods.

This training must include, but is not limited to:

- All Company information security policies, procedures and standards and/or significant revisions to them.
- The secure use of Company information systems (e.g. log-on procedures, authorized software).
- Significant risks to Company information systems and data and/or any new threats as they are identified.
- The Company's legal and business responsibilities for protecting its information systems and data. (e.g. HIPAA, business associate contracts) and/or any significant changes to these responsibilities.
- Security best practices (e.g. how to construct a good password, how to report a security incident) and/or changes to these practices.
- Security controls in place, any changes to these controls, and/or new controls being implemented.

As part of this training, Company employees and individuals associated with the Company must read, confirm their understanding, and agree to comply with the written information security program (“WISP”) prior to receiving access to Company information systems.

## WRITTEN INFORMATION SECURITY PROGRAM (WISP)

### SECURITY AWARENESS TRAINING POLICY

<<Legal Entity>> (TEMPLATE – Smaller Entity)

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

**Effective Date:** << INSERT DATE >>

Company employees and individuals associated with the Company must receive appropriate security training and after such training, each employee must verify that he or she has received the training, understood the material presented, and agree to comply with it.

All Company information security policies and procedures must be readily available for reference and review by appropriate employees, business associates and individuals associated with the Company.

All Company workforce members responsible for implementing safeguards to protect information systems must receive formal training that enables them to stay abreast of current security practices and technology