## 1.0 PURPOSE

The purpose of this Policy is to provide a security framework that will ensure protection of (Client Name)'s information from unauthorized access, loss, or damage while supporting the open, information-sharing needs of our Company (Client Name) information may be verbal, digital, and/or hardcopy, individually controlled or shared, stand-alone or networked, and used for different purposes.

(Client Name) President delegates to Company management the development and approval of Standards and procedures related to, and used to enforce, this Information Security Policy.

Any Company employee found to have violated this policy may be subject to disciplinary action according to Company Human Resources policies. This could include formal reprimands up to and including termination of employment based on management's discretion. Criminal activities may be forwarded to appropriate law enforcement authorities within the State of Connecticut. Failure to enforce this policy in response to possible violations shall not be deemed a waiver of management's right to enforce the policy with respect to any other violations.

## 2.0 SCOPE

This information security Policy includes recommendations as issued by the FFIEC, Information Technology (IT) security requirements from the National Institute of Standards and Technology (NIST), Special Publication (SP) NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations; the privacy requirements of the General Data Protection Regulation (GDPR) of the European Union (EU), other regulatory and mandated guidance; and other sources. Additionally, this policy applies to all employees, temporary employees, interns, contractors, vendors, and all information systems to include those owned or leased by (Client Name).

Information is one of the Company's key assets and needs to be suitably available and protected, for the Company to achieve our strategic goals. The Company shall take all necessary steps to protect this information from internal, external, deliberate or accidental threats. To achieve this objective, this policy establishes the foundation for Company efforts and activities and provides information security direction. It is based on the following three principles: Confidentiality, Integrity, and Availability.

- **Confidentiality** – Ensuring that information is kept in strict privacy.
- **Integrity** – Ensuring the accuracy, completeness, and consistency of information.
- **Availability** – Ensuring that information is ready and suitable for use whenever needed.

Other definitions pertaining to this policy include:

- **Policy** – A guiding principle used to set direction.
- **Standard** – A mandatory action or rule designed to support and conform to a policy.
- **Procedure** – Series of steps to be followed as a consistent and repetitive approach to accomplish a result.
- **Information** – Data that is accurate and timely, and valuable to the Company.

- **Information System** – This is the Company's hardware (servers, workstations, printers, etc.); software; applications; databases; and/or network infrastructure that processes, transmits, or stores Company information.
- **Authorization** – the function of establishing an individual's privilege levels to access and/or handle information.
- **Unauthorized Access** – looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need.
- **(Client Name) Information** – information that the Company collects, possesses, or has access to, regardless of its source. This includes electronic data, information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

(Client Name) standard and baseline for information security within the Company shall be recommendations as issued by the FFIEC, U.S. National Institute of Standards and Technology (NIST) minimum requirements; the privacy directives within the General Data Protection Regulation (GDPR) of the European Union (EU); (Client State Location) State law; and where applicable, Payment Industry Standards; as well as other governmental laws and regulations. Information security policy, standards, and procedures shall be documented as follows:

- The Information Security Policy (ISP) document provides overall information security guidance for the Company;
  - The Company specifies adopted controls, and hence, documents the detailed security policy that the Company has chosen to mitigate the assessed risks in our information systems;
- The Acceptable Use of IT Resources provides the users of Company information systems with clear guidelines on what is permitted/not permitted while using these systems;

Detailed security requirements for specific technologies and/or systems are detailed in technical Standards, which are used together with supporting procedures for the management and maintenance of systems' security. Technical Information Security-Related Standards include:

- The Access Control Security Standard that provides the users of Company information systems with clear requirements on how access to Company information systems and data is controlled;
- The Audit and Accountability Security Standard that provides clear requirements for how Company information systems capture system and behaviour-related events, and how Company employees will review, analyse, and report on any actionable events;
- The Identification and Authentication Security Standard that provides the users of Company information systems with clear requirements for identifying themselves, and authenticating to Company information systems;
- The System Communications and Protection Security Standard that provides clear requirements on how the Company shall protect our data and information systems;

Detailed security requirements for specific Company security operations are detailed in operational Standards, which are used together with technical Standards for the management and maintenance of the Company network and security architecture. Operational Security-Related Standards include:

- The Security Awareness and Training Standard that addresses requirements for security awareness training, role-based security training, and maintaining training records;

- Adequate and appropriate security awareness programs shall be conducted in order to ensure that Company information security policies and standards are understood and followed by Company personnel and relevant stakeholders;

- The Configuration Management Security Standard that defines and addresses the different configuration management elements such as, configuration baselines; configuration change control procedures; and how system flaws are mitigated, and remediated;
- The Incident Response Security Standard that describes how the Company responds and manages incidents that could impact the security of the Company;
- The Maintenance Security Standard that describes how Company information systems are to be maintained internally, and by third parties;
- The Media Protection Security Standard that describes how the Company will protect information stored on remote devices such as USB drives, external hard drives, DVD-ROM's, etc. and how media are to be secured, or destroyed;
- The Physical Protection Security Standard that describes how the Company will protect personnel, facilities, and information systems from environmental and/or man-made threats;
- The Personnel Security Standard that includes the Human Resources (HR) Standard which addresses how personnel access needs are to be evaluated before gaining access to Company information systems and/or information;
- The System and Information Integrity Security Standard that describes how the Company protects the information systems and data from internal and external threats.

Management Information Security-Related Standards include:

- The Risk Assessment Security Standard which addresses requirements on how to identify, mitigate, remediate, and manage risks at the Company, and on Company information systems; and
- The Security Assessment Standard that describes how the Company will assess the implementation of security controls, through vulnerability scanning, security controls assessments, penetration testing, etc.

All employees will be provided with the Acceptable Use of IT Resources Standard, to which they will be obligated as part of their employment with (Client Name).

## 3.0 CLASSIFICATION LEVELS

All Company information is classified into one of two levels based on its sensitivity and the risks associated with disclosure. These classification levels determine the security protections that must be used for the information. When combining information, to manage risks, the classification level of the resulting information must be re-evaluated independently of the source information's classification. The three classification levels include: Restricted, and Internal as well as other, unmarked data which are assumed to be General Use.

- Restricted includes:
  - Social security number
  - Bank account number
  - Driver's license number
  - State identity card number
  - Credit card number

  - Information contained in personnel files
  - Misconduct and law enforcement investigation records
  - Internal financial data
  - Product cost data
  - Protected health information (as defined by HIPAA)
  - Model numbers (both design and production)
- Internal
  - Unrestricted email
  - Otherwise unrestricted internal memos
  - General correspondence
- General Use includes:
  - Information that is intended to be made available to anyone inside or outside of the Company.

## 4.0 GOVERNANCE

To achieve sustainable management of information security the Company shall appoint a person who will fulfill the Company's Security Manager Role, having appropriate levels of authority for the function.

The Security Manager is accountable for all information security related to the Company's Information Systems.

The Security Manager is responsible for monitoring, enforcing and reviewing Company Information Systems for compliance with information security policies, and producing regular management reports on the status of information security within the organization. He/she is also responsible for ensuring that Company information security policies are regularly reviewed and updated as necessary.

The following departments within the Company have specific roles in maintaining information security within the organization:

- The Company Human Resources (HR) department is responsible for ensuring employees are aware of their obligations regarding Information Security and for providing appropriate security orientation training for employees;
- The Company Maintenance department is responsible for ensuring the physical security of Company owned, leased or operated properties;
- The Company Information Technology (IT) department is responsible for implementing Company Information Security policies and standards for Company Information Systems and to carry out daily security operations;
  - The Company IT department is also responsible for ensuring Company Information Systems are monitored for security risks. Additionally, the Company IT department will ensure that an independent audit of Information Systems is conducted annually.

Other Company directors and managers shall be responsible for ensuring the Company's information security policies are implemented and complied with for current and future Company Information Systems under their management.

## 5.0 REFERENCES

The following security-related documentation shall be used when enforcing the Information Security Policy:

- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED

## 6.0 APPROVALS

Signature

Name

Title

Date

Signature

Name

Title

Date