Initek Information Security Policy

Policy Title: Information Security Policy
Responsible Executive: CISO, Eric Somogyi
Responsible Office: Office of Information Technology, Information Security Office
Contact: Chief Information Security Officer, Eric Somogyi
Effective Date: First version: October 6, 2024;
Last Update: October 8, 2024

1. Policy Statement

The purpose of this policy is to provide a security framework that will protect the company from all internal and external threats while ensuring the protection of Initek's Company Information from unauthorized access, loss or damage, while supporting the information sharing of our company.[3]

2. Scope

This policy applies to all employees, contractors, vendors and third-party entities who access, handle, or manage Initek's information systems, networks, applications, and data.[4]

3. Definitions

Cybersecurity risk appetite – the amount and type of risk that Initek is willing to tolerate in pursuit of its objectives.

Information security - the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability. [1]

Initek Company Information – Information that Initek collects, possess, or has access to, regardless of its source. This includes information contained internally on the company servers or external servers, hard copy documents, any kind of media, and any data collected from voice communications or data networks, or exchanged in conversation. [5]

Unauthorized Access - looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need, regardless of who the entity, employee, or person is. [6]

4. Who is Affected By This Policy

The Information Security Policy applies to all Initek employes and Initek customers. This policy also applies to all other individuals and entities granted use of Initek Company Information, including, but not limited to, contractors and third party vendors.

5. Purpose

The purpose of this policy is to ensure that Initek and its employees here onwards implement appropriate measures to maintain confidentiality, protect the integrity and improve the availability of Initek's information assets through the organization and creation of a security program and policies, which would result in a reduction in data breaches and reduction in management relating to technical vulnerabilities.

This policy aligns with compliance requirements based on the NIST Cybersecurity Framework and also Initek's customer contractual obligations.

Initek recognizes that this information security policy will help and support Initek in achieving business objectives by reestablishing trust with customers, business partners, and staff while ensuring compliance with applicable statutory, regulatory, and customer requirements and while complying with Sarbanes Oxley and HIPAA.

This Information Security Policy helps define how employees and management will properly handle potential events and incidents relating to the company's information assets culture within the organization that fosters.

The implementation and enforcement of this policy will assist Initek's and achieving strategic goals while meeting the company's cybersecurity risk appetite.

This policy provides the controls that will be used to achieve company-wide security during information sharing through encryption techniques and access controls as the enabling mechanism for information sharing.

The Policy of Initek is on a continuing basis to protect Information Systems with due diligence to securely handle company assets from *unauthorized access*, use, disclosure, or modification. This will ensure that we are aligned with our business objectives.

6. Statement of Management Intent

The Policy of Initek is on a continuing basis to protect Information Systems with due diligence to securely handle company assets from *unauthorized access*, use, disclosure, or modification. This will ensure that we are aligned with our business objective of re-establishing trust with our customers is maintained.

The management team bears the responsibility overseeing employees with significant responsibilities and will make sure that employees are adequately trained.

Initek has an issue-specific Policy of *Internet Access* which will address those who will have access to certain types of systems connected to the network. This Policy will be made available to all employees within the company, so each employee has a proper understanding of what is required of them.

Initek has a system-specific Policy that will dictate the appropriate security configurations for employees implementing the security controls relating to malware and secure handling of encrypted assets. [2]

Initek has a Policy of Continual Improvement in line with the NIST Cybersecurity Framework requirements.

In order to ensure that Initek meets the compliance requirements of Sarbanes Oxley and HIPAA, the information systems and company resources will be managed with an acceptable level of risk, which has been agreed by Initek's internal stakeholders, while also meeting Initek's customers' contractual obligations.

7. Security Principles, Standards, and Compliance Requirements

Initek is committed to ensuring the confidentiality, integrity, and availability of its information assets based on industry-recognized frameworks. As stated earlier in our Purpose, our approach is to meet legislative, regulatory, and contractual obligations, while providing security education using the budget we have allocated for educational awareness.

Framework that the Policy is Based On

This policy is based on the NIST Cybersecurity Framework (CSF) 2.0 which allows us to identify, protect, prevent, and correct cybersecurity incidents or accidents with our goals and objectives.

Standards Defined in Our Control Framework

Security controls defined in this framework include:

- Initek has an issue-specific Policy of *Internet Access* which will address those who will have access to certain types of systems connected to the network. This Policy will be made available to all employees within the company, so each employee has a proper understanding of what is required of them.
- Policy for Information Security: An information security policy document is approved by management, published and communicated to all employees and relevant external parties.
- Controls against malware: Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.
- Handling of Assets Data Protection (Encryption): Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.
- Management of technical vulnerabilities: Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.
- Logging and Monitoring of events: Documented evidence of security-relevant activities being logged and included as part of the centralized event log collection and review/analysis process.

Compliance with Legislative, Regulatory, and Contractual Requirements

Initek complies with several frameworks and customer contractual obligations which include, but are not limited to:

- **Sarbanes-Oxley Act of 2022 (SOX)**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **Customer Contracts**

Security Education, Training, and Awareness Requirements

All employees, contractors, and third parties are required to complete a 30-day training program within getting hired or signing any service level agreement (SLA). Security training includes:

- Annual security awareness training to educate and update all personnel on the latest safety practices and Initek security policies.
- Software and Hardware Training is mandatory to all current employees and is available based on roles within the company.

8. Policy Review

At a minimum, the Information Security Policy will be reviewed weekly.

9. Update Log

September 1, 2024 – Policy issued.
October 1, 2024 – Approved by Initek Board..
October 8, 2024 – Policy updated.

10. Sources

1 NIST Special Publication 800-12 Revision 1 - *An Introduction to Information Security* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf (page 2).

2 NIST Special Publication 800-12 Revision 1 - *An Introduction to Information Security* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf (page 31)

3 Princeton Office of Information Security - *Information Security Policy* – Purpose statementhttps://oit.princeton.edu/policies/information-security

4 Information Security Template – Scope "sentence" https://www.business-in-a-box.com/template/information-security-policy-D13552/

5 Princeton Office of Information Security - *Information Security Policy* – Company Information Definition https://oit.princeton.edu/policies/information-security