Made from the template at https://frsecure.com/information-security-policy-template/

FRSECURE

Information Security Policy, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document Owner: Information Security Committee
Last Review Date: August 2020

Information Security Policy

Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the I-Dunno Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

- Confidentiality – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic "need to know" principle.
- Integrity – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
- Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

I-Dunno has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security policies may be developed to ensure that the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to I-Dunno by its stakeholders, partners, customers and other third parties.

The I-Dunno Information Security Program is built around the information contained within this policy and its supporting policies.

Purpose

The purpose of the I-Dunno Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to I-Dunno, its business partners, and its stakeholders.

Audience

The I-Dunno Information Security Policy applies equally to any individual, entity, or process that interacts with any I-Dunno Information Resource.

Responsibilities

Executive Management

- Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of I-Dunno.
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.
- Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.
- Ensure that the Security Team is given the necessary authority to secure the Information Resources under their control within the scope of the I-Dunno Information Security Program.
- Designate an Information Security Officer and delegate authority to that individual to ensure compliance with applicable information security requirements.
- Ensure that the Information Security Officer, in coordination with the Information Security Committee, reports annually to Executive Management on the effectiveness of the I-Dunno Information Security Program.

Information Security Officer

- Chair the Information Security Committee and provide updates on the status of the Information Security Program to Executive Management.
- Manage compliance with all relevant statutory, regulatory, and contractual requirements.
- Participate in security related forums, associations and special interest groups.
- Assess risks to the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of I-Dunno.
- Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.
- Ensure that I-Dunno has trained all personnel to support compliance with information security policies, processes, standards, and guidelines. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities.
- Ensure that appropriate information security awareness training is provided to company personnel, including contractors.
- Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of I-Dunno.
- Develop and implement procedures for testing and evaluating the effectiveness of the I-Dunno Information Security Program in accordance with stated objectives.
- Develop and implement a process for evaluating risks related to vendors and managing vendor relationships.
- Report annually, in coordination with the Information Security Committee, to Executive Management on the effectiveness of the I-Dunno Information Security Program, including progress of remedial actions.

Information Security Committee

In accordance with the Information Security Committee Charter:

- Ensure compliance with applicable information security requirements.

- Formulate, review and recommend information security policies.
- Approve supporting procedures, standards, and guidelines related to information security.
- Assess the adequacy and effectiveness of the information security policies and coordinate the implementation of information security controls.
- Review and manage the information security policy waiver request process.
- Identify and recommend how to handle non-compliance.
- Provide clear direction and visible management support for information security initiatives.
- Promote information security education, training, and awareness throughout I-Dunno, and initiate plans and programs to maintain information security awareness.
- Educate the team and staff on ongoing legal, regulatory and compliance changes as well as industry news and trends.
- Identify significant threat changes and vulnerabilities.
- Evaluate information received from monitoring processes.
- Review information security incident information and recommend follow-up actions.
- Report annually, in coordination with the Information Security Officer, to Executive Management on the effectiveness of the I-Dunno Information Security Program, including progress of remedial actions.

All Employees, Contractors, and Other Third-Party Personnel

- Understand their responsibilities for complying with the I-Dunno Information Security Program.
- Formally sign off and agree to abide by all applicable policies, standards, and guidelines that have been established.
- Use I-Dunno Information Resources in compliance with all I-Dunno Information Security Policies.
- Seek guidance from the Information Security Team for questions or issues related to information security.

Policy

- I-Dunno maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures and guidelines that:
    - Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical and technical controls.
    - Provide value to the way we conduct business and support institutional objectives.
    - Comply with all regulatory and legal requirements, including:
        - HIPAA Security Rule,
        - State breach notification laws,
        - PCI Data Security Standard,
        - Information Security best practices, including ISO 27002 and NIST CSF,
        - Contractual agreements,
        - All other applicable federal and state laws or regulations.
- The information security program is reviewed no less than annually or upon significant changes to the information security environment.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 5, 6, 7, 18
- NIST CSF: ID.AM, ID.BE, ID.GV, PR.AT, PR.IP
- Information Security Committee Charter

Waivers

Waivers from certain policy provisions may be sought following the I-Dunno Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	August 2020		FRSecure	Document Origination

NEED HELP?

FRSecure is a full-service information security consultancy.

If you need assistance with anything in this resource, please don't hesitate to reach out to us.

CONTACT US

(877) 767 – 1891 | 6550 York Ave S #500, Edina, MN 55435

For security emergencies, or quotes on services **reach out to us here**.

More resources