INFORMATION SECURITY POLICY

INTRODUCTION:

Information Security Policy is a foundational document that outlines an organization's approach to safeguarding its information assets. In today's interconnected and digital world, where data is a critical asset, organizations need a comprehensive framework to manage and protect their information. Information Security Policies serve as the cornerstone of this framework, providing guidelines, rules, and procedures to ensure the confidentiality, integrity, and availability of sensitive information.

* 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.

PURPOSE:

The purpose of an Information Security Policy is multifaceted, encompassing various objectives aimed at safeguarding an organization's information assets.

AUDIENCE:

An Information Security Policy includes various stakeholders within an organization who play different roles in ensuring the security of information. The policy is designed to communicate guidelines, responsibilities, and expectations regarding information security.

**RESPONSIBILITIES:**

Executive Management:

* CEOs, CFOs, CIOs and other top-level executives who are responsible for overall organizational strategy and decision-making.
* Executive leadership needs to understand the importance of information security in achieving business objectives and ensuring the organization’s resilience against cyber threats.

IT Security Teams:

* Chief Information Security Officers (CISOs), IT managers, network administrators, and security professionals responsible for implementing and maintaining information security measures.
* These teams need clear guidance on security controls, incident response and technology-specific policies to secure the organization’s IT infrastructure.

Employees:

* Employees need to be aware of their roles and responsibilities in safeguarding information, understanding security best practices, and recognizing potential security threats.

Human Resources Department:

* HR professionals are responsible for ensuring that employees are aware of and adhere to the information security policy.
* HR may also play a role in onboarding and offboarding employees with respect to information security policies and practices.

Legal and Compliance Teams:

* Legal and compliance professionals ensure that the organization adheres to relevant laws, regulations, and industry standards.
* These teams play a critical role in ensuring that the Information Security Policy aligns with legal requirements and compliance obligations.

Auditors and Compliance Accessors:

* Internal and external auditors, as well as compliance assessors, who evaluate the organization's adherence to information security policies.
* These stakeholders use the policy as a benchmark for assessing the organization's compliance with security standards.

Third Party Vendors and Partners:

* The policy may include guidelines for third parties to adhere to security standards and practices when interacting with the organization's information.

Customers and Clients:

* Depending on the nature of the business, customers and clients may be interested in understanding the organization's commitment to information security.
* Transparency about security measures can build trust and confidence among customers.

Board of Directors:

* Members of the board who oversee corporate governance and risk management.
* The board needs to be informed about the organization's information security posture and how it aligns with the overall risk management strategy.

**POLICY:**

[Company Name] is committed to maintaining a robust Information Security Program to safeguard the Confidentiality, Integrity, and Availability of Information Resources. This program includes a comprehensive set of policies, standards, procedures, and guidelines.

Our primary objectives are to:

* Protect the Confidentiality, Integrity, and Availability of Information Resources.
* Implement administrative, physical, and technical controls to ensure effective security measures.
* The Information Security Program is designed to provide tangible value to our business operations, supporting and aligning with institutional objectives.
* Our Information Security Program adheres to all relevant regulatory and legal requirements, including:
* HIPAA Security Rule
* State breach notification laws
* PCI Data Security Standard
* Information Security best practices (ISO 27002 and NIST CSF)
* Contractual agreements
* All other applicable federal and state laws or regulations.
* The Information Security Program undergoes a thorough review at least annually. Additional reviews are conducted upon significant changes to the information security environment to ensure its ongoing effectiveness.

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.