Information Security Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Policy ID |  | **Effective Date** | Date |
| Version | 1.0 | **Contact** |  |
| Scope | All Firm PersonnelThird-Party Vendors |  |  |

**Table of Contents**

1.0 Overview 1

2.0 Purpose 1

3.0 Scope 1

4.0 Definitions 2

5.0 Vision & Goals 2

6.0 Roles & Responsibilities 2

7.0 Organization of Information Security Policies 3

7.1 Supporting Policies & Audience 3

8.0 Information Protection and Usage 3

9.0 Reporting Policy Legal Conflicts 4

10.0 Compliance & Violation 4

11.0 Vendor Management 4

12.0 Client Contractual Agreements (related to security and data handling) 4

13.0 Exceptions to Policies 4

Revision History 4

# 1.0 Overview

It is the policy of Firm Name that information, as defined hereinafter, in all its forms – written, spoken, electronic, or printed—will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information. This policy will be supported by other security-related policies and technology acceptable use policies published by Firm Name.

The Firm routinely monitors its systems and usage patterns. In addition, to the maximum extent permitted by law, the Firm, at any time in its sole discretion, reserves the right to monitor, log, search, access, read and examine any and all information created, stored or received on, or passing through, Firm systems and devices. Such examination may be undertaken in general and/or to: help ensure compliance with internal policies; support the performance of internal investigations and incident response; or collect information responsive to a court order, a litigation discovery request, a subpoena or a government inquiry. Firm Name reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

# 2.0 Purpose

This Information Security policy is intended to provide the framework to ensure the confidentiality, integrity, and availability of data and resources through the use of effective and established processes and procedures.

# 3.0 Scope

This policy applies to all Employees, Non-Partner Attorneys, Partner Attorneys, and external vendors who have or are responsible for an account on any system that resides in Firm Name’s environment, or managed systems in the cloud.

# 4.0 Definitions

**Availability**: Data or information is accessible and usable upon demand by an authorized person.

**Confidentiality**: Data or information is not made available or disclosed to unauthorized persons or processes.

**Encryption**: The process of converting data into a code to read encrypted data, a secret key is needed to "unlock," or convert, the data into readable form. Encrypted data is referred to as ciphertext, and unencrypted data is called plaintext.

**Information**: Can exist in many forms – printed or written on paper, stored electronically in files or databases, transmitted by post or electronically, shown on video, or spoken in conversation. The information security program protects the firm’s client information, attorney work product and corporate information.

**Information Security:** The preservation of confidentiality, integrity, and availability of information stored, processed, and transmitted by the Firm.

**Information Security Program** : Governance system by which the firm’s information security activities are directed and controlled.

**Integrity**: Data or information has not been altered or destroyed in an unauthorized manner.

# 5.0 Vision & Goals

All client information will, at all times, be responsibly protected against all threats.

Firm Name is committed to ensuring information security is an ongoing integral part of the Firm’s business and strategic planning. The principles and objectives in this section communicate the vision for managing the Firm’s information security.

| **Principle** | **Objective** |
| --- | --- |
| Comply with relevant legal and regulatory requirements. | Ensure that statutory obligations are met, stakeholder expectations are managed, and civil or criminal penalties are avoided. |
| Protect confidential information. | Prevent disclosure of confidential information to unauthorized individuals. |
| Act in a professional and ethical manner. | Ensure that information security-related activities are performed in a reliable, responsible and effective manner. |

# 6.0 Roles & Responsibilities

1. **Security Team/Leads**: A team, comprised of the Chief Information Officer, Chief Operating Officer, and IT Manager, responsible for developing and implementing security policies, procedures, and controls, subject to the approval of Firm Name management. This team has overall responsibility for the firm’s information security program and serves as a liaison between executive management (i.e., Management Committee) and the program. The Security Team is accountable for establishing security risk tolerance levels, defining and implementing security risk assessment and treatment strategies, and reviewing security risk assessments.
2. **Security Manager**: User Support & Process Improvement IT Manager will have overall responsibility for management of the Firm’s information security efforts under the direct and close supervision of the Chief Information Officer.
3. **Information Owner**: The owner of a collection of information is usually the manager responsible for the creation of that information or the primary use of that information. For client information, the Information Owner is the Client Responsible Attorney.
4. **Custodian**: The custodian of information is generally responsible for the processing and storage of the information. Custodians include members of Networking, Application Support, Financial Application Support, and Litigation Support. The custodian is responsible for the administration of controls as specified by the owner.
5. **User**: The user is any person who has been authorized to read, enter, or update information. A user of information is expected to comply with any supporting Security Policies and procedures.

# 7.0 Organization of Information Security Policies

The firm’s information security policies are organized into three levels: core policy (this document), supporting policies and supporting procedures for practice areas and administrative teams.

## 7.1 Supporting Policies & Audience

|  |  |
| --- | --- |
| Audience | Supporting Policies |
| All | * Information Classification
* Password
* Vendor Management
* Data Handling
* Working Remotely
* Security Incident Reporting
 |
| Management | * Information Security Program
* Incident Response
 |
| Technology Services | * Account Management
* IT Asset Management
* Encryption Management
* Malicious Software Management
 |

# 8.0 Information Protection and Usage

1. Firm Name and its client information must be consistently protected in a manner proportionate with its sensitivity, value, and criticality. See *Information Classification Policy.*
2. All access to, uses of, and processing of, Firm Name and client information must be consistent with Firm Name policies and standards.
3. This policy applies regardless of the media on which information is stored, the locations where the information is stored, the systems technology used to process the information, or the people who handle the information.
4. Firm Name information must be used only for the business purposes expressly authorized by management.
5. Client information must be used only for the business purposes expressly authorized by the nature of the matter and by the client.
6. Protected information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.
7. All non-approved uses of both client and Firm Name information are prohibited.

# 9.0 Reporting Policy Legal Conflicts

1. Firm Name information security policies are drafted to meet or exceed the protections found in existing laws and regulations, and any Firm Name information security policy believed to be in conflict with existing laws or regulations must be promptly reported to the Security Team.

# 10.0 Compliance & Violation

1. Management’s non-enforcement of any policy requirement does not constitute its consent.
2. Any users with access to the information outlined within this document that are aware of any incidents of loss, breached, or compromised information shall report immediately to the Security Team.

# 11.0 Vendor Management

1. Any vendor providing services or having access to the Firm’s information shall be subject to the same security standards with this policy and supporting policies.
2. Prior to gaining access to Firm Name systems or information, the steps outlined within the *Vendor Management Policy* must be followed.

# 12.0 Client Contractual Agreements (related to security and data handling)

1. All client agreements related to the storage, processing, and handling of client information, as well as any specific security standards, should be reviewed, at a minimum, by the Security Team.
2. Execution of such agreement can only be finalized once a formal review is complete.

# 13.0 Exceptions to Policies

1. Exceptions to information security policies must be brought to the Security Team for approval.

# Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review Date | Reviewer/ApproverName |
| 1.0 | Initial Version |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |