Information Security
Data Handling Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Policy ID |  | **Effective Date** |  |
| Version | 1.0 | **Contact** |  |
| Scope | EmployeesNon-Partner AttorneysPartner AttorneysThird-Party Vendors |  |  |

**Table of Contents**

1.0 Overview 1

2.0 Purpose 1

3.0 Scope 1

4.0 Definitions 1

5.0 Access to Information 2

6.0 Information Exchange/Transportation 2

7.0 Storage of Information 3

8.0 Disposal of Information and Media 3

9.0 Related Policies 3

10.0 Policy Maintenance 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.

# 2.0 Purpose

The objective of this policy is to maintain the security of information handled within the organization and with any external entity.

# 3.0 Scope

This policy applies to all Employees, Non-Partner Attorneys, Partner Attorneys, and 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.

**HIPAA**: The Health Insurance Portability and Accountability Act, a federal law passed in 1996 that affects the healthcare and insurance industries. A key goal of the HIPAA regulations is to protect the privacy and confidentiality of protected health information by setting and enforcing standards.

**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.

**Protected Health Information (PHI)**: PHI is health information, including demographic information, created or received from a covered entity which relates to the past, present, or future physical or mental health or condition of an individual; or the past, present, or future payment for the provision of health care to an individual and that identifies or can be used to identify the individual.

**Portable Media Device**: Any computing device or peripheral that can be carried and can have information stored upon it. (Examples include: CDs, USB Flash Drives, Smartphones, etc)

**Personally Identifiable Information (PII)**: Information about an individual that could reasonably be used to identify them, such as their name, fingerprints, email address, or social security number. PHI and PIFI are subtypes of PII.

**Protected Information**: Information that is protected by local, state, and federal regulations (i.e., HIPPA).

# 5.0 Access to Information

1. Firm Name uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, management maintains the authority to: (1) restrict or revoke any user's privileges, (2) inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and (3) take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users. Firm Name disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.
2. Protected Information, as outlined in the *Information Classification Policy*, should be restricted only to the information users (i.e., Matter Team) with a legitimate need to carry out the legal service.
3. Access to data with restricted access (i.e., restricted workspaces in Document Management System, delegate access to Outlook mailbox) must have documented request and approval from information owner.
4. User desktops must be secured against use by unauthorized individuals.
5. Servers and other infrastructure equipment must be installed in an access-controlled area. The area in and around the facility must contain protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.

# 6.0 Information Exchange/Transportation

1. When using portable media (i.e., flash drives, CDs) for Internal, Confidential or Protected classified information, encryption technology must be used.
2. Individuals transporting portable devices or media off-site must be proficient in the use of appropriate security controls (i.e., encryption) for those devices.
3. When transferring Protected or Confidential information through online file sharing services, the use of the Firm-approved system (i.e., ShareFile) is required.
	1. Exceptions to the Firm-approved system must be mutually agreed upon, in writing, with the client. An email is an acceptable form of agreement.
4. Acceptance or request of any information containing PHI or PII should be avoided unless such information is relevant to providing legal or administrative services.
5. Mass data transfers of Confidential and Protected information shall follow processes outlined in the Firm’s Records Retention Policy.
6. Appropriate privacy/security agreements must be in place with any vendor to which physical media devices are transferred to the custody of the vendor.
7. Carriers transporting media/devices must protect information assets from unauthorized discloser and provide a formal record of transfer and its receipt at the destination (firm-employed or contracted 3rd party).

# 7.0 Storage of Information

1. Firm Name and client information should be stored into systems (i.e., Document Management System) which employ complete redundancy and appropriate backups to ensure information availability.
2. Protected and Confidential information must never be stored on mobile computing devices (laptops, tablets, smartphones), unless the devices have the following minimum security requirements implemented:
	1. Device Passwords
	2. Auto Logoff or screensaver with password
	3. Encryption of stored data or other acceptable safeguards approved by the Information Security Team.
3. Protected and Confidential information stored on portable/external media (i.e., CDs, USB flash drives) must be protected from theft and unauthorized access. Such media should be labeled appropriately and never left unattended in unsecured areas.
4. Storage of any information of PHI or PII is prohibited unless:
	1. It serves legitimate purpose in providing a legal service or administrative function.
	2. The information is restricted to only those with a legitimate purpose to use that information.
5. Any assets (laptops, portable media, smartphones, etc) assigned to employees to which contain Firm Name or client information are the responsibility of the employee to maintain an appropriate level of security. Such information should only be stored on devices temporarily and properly moved to permanent Firm resources/systems.
6. Firm or client data should not be stored in public- or cloud-based environments or repositories that are not authorized by the Firm.
7. Using web-based or third-party services to backup, store, copy, or synchronize Firm or client data is prohibited.
8. Retention of information shall follow the Firm’s Record Retention Policy.

# 8.0 Disposal of Information and Media

1. IT assets storing Firm or Client information must be disposed of following the *IT Asset Management Policy*.
2. Portable devices and electronic media should a) be disposed of appropriately, or b) returned to the client/outside party in a timely fashion if the original device was provided by the client.

# 9.0 Related Policies

* Information Classification
* IT Asset Management
* Records Management
* Technology Acceptable Use

# 10.0 Policy Maintenance

The responsibility of ensuring this policy is kept current as needed for purposes of compliance with the Firm’s security requirements is assigned to the Security Team.

### Revision History

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