Information Security
Vendor Management Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Policy ID |  | **Effective Date** |  |
| Version | 1.0 | **Contact** |  |
| Scope | Firm |  |  |

**Table of Contents**

1.0 Overview 1

2.0 Purpose 1

3.0 Scope 1

4.0 Elements of Risk 2

5.0 Due Diligence 2

6.0 Contractual Documentation 2

7.0 Vendor Access Control 3

8.0 Information Exchange 3

9.0 Related Policies 3

10.0 Related Form 3

11.0 Policy Maintenance 3

Revision History 3

# 1.0 Overview

In accordance with the Firm’s internal security practices and requirement; and those requirements mandated by the Firm’s clients, Firm Name has established a formal Vendor Management policy and supporting procedures.

Proper vendor management means conducting due diligence in vendor selection, and reviewing all necessary contractual documentation upon engagement of vendor services.

Additionally, the term “vendors” is defined as an entity providing outsourcing services to Firm Name. Whereas, “third-party” is defined as a vendor of the Firm’s vendor.

# 2.0 Purpose

The purpose of this policy is to set forth a formalized Vendor Management policy that is to be adhered to and utilized throughout the Firm at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of Firm Name system resources and information.

# 3.0 Scope

This policy and supporting procedures encompasses all vendors who store/maintain/interact with systems and information that are owned, operated, or maintained by Firm Name and all other system resources, both internally and externally.

Internal systems owned, operated, and maintained by the Firm, all network devices (firewalls, routers, switches, etc) servers (physical and virtual), and any other system resources are deemed in scope.

External system resources owned, operated, and maintained by any entity other than Firm Name, but for which these very resources may impact the confidentiality, integrity, availability, and overall security of the aforementioned description of “Internal System Resources”.

# 4.0 Elements of Risk

When using the services of various vendors, a certain element of risk arises. It is important to understand these risks, what they are, and how Firm Name can readily identify any issues, concerns, or constraints pertaining to these risks.

1. **Compliance Risk** – Risks arising from violations of applicable laws, rules, and regulatory mandates (i.e., PII, HIPAA).
2. **Strategic Risk** – Risks arising from vendors failing to implement business initiatives that align with the overall goals of Firm Name, such as not offering an acceptable return on investment.
3. **Operational Risk** – Risks arising from a failed system of operational controls related to uptime.
4. **Information Technology Risk** – Risks arising from any number of information technology and information security issues, such as inadequate IT resources.
5. **Financial Risk** – Under the discretion of Senior Management or the decision maker; and/or involvement of a “mission critical” system – a financially stable entity is of upmost importance.

# 5.0 Due Diligence

The selection process for new vendors consist of certifying all the relevant aforementioned risk areas have been thoroughly identified by Firm Name, which may include the following measures:

* Collection of all regulatory compliance and operational audits and assessments.
* Experience and overall business “know-how”.
* Operational capacity and scalability.
* Use of other third-parties by the vendors themselves.
* Reputation within the industry.
* Gathering of operational, business specific, and information security policies, procedures, and practices (i.e., incident response, security awareness, business continuity, and disaster recovery planning).
* Cyber Insurance coverage.

# 6.0 Contractual Documentation

Once vendors have been selected for providing critical outsourcing services to Firm Name, the following procedures are to be undertaken regarding contractual documentation:

* A formalized and written contract has been produced including identification of roles, responsibilities, obligations, and expectations from all relevant parties.
* The contract has been approved by a member of senior management of the Firm which may also include key stakeholders.
* Information security protection measures appropriately documented.
* Non-Disclosure Agreement (NDA) has been signed for any Vendor with visibility to the Firm’s information.
* If vendor stores/processes Firm Name information through a cloud solution, an Exit Strategy may need to be clearly defined in the event the services are no longer needed. Under the discretion of senior management, this may include language in the return of firm information, or the certifiable destruction of that data.
* Stipulations included that the vendor must notify the Firm immediately of any security incident likely to impact sensitive Firm information under their control.
* All contracts with web site hosting organizations, application service providers, managed systems security providers, and other information systems outsourcing organizations must include both a documented backup plan and a periodic Vendor testing schedule.
* Agreements with vendors, such as suppliers, service providers, and business partners, which could negatively impact the business processes of the Firm must define service level agreements and require minimum standards of contingency planning and preparation on the part of the vendor.
* Vendors hold their vendors (third-parties) to the same standards.

# 7.0 Vendor Access Control

* Vendor access to any Firm internal computer systems that are not clearly public must be approved in advance by a designated Information Security Team member.
* A UserID, password, and two-form authentication token will be assigned in respects to the *Account Management Policy*.

# ****8.0 Information Exchange****

* **Vendor Sensitive Information Handling** - All disclosures of Confidential and Protected information to vendors must be accompanied by an explicit statement describing exactly what information (type of information) is restricted and how this information may and may not be used.
* **Vendor Non-Disclosure Agreements** - Prior to sending any Firm information to a vendor for copying, printing, formatting, or other handling, the vendor must sign a non-disclosure agreement.
* **Vendor Security Policy** - Before any Firm information is disclosed to a vendor, the vendor must submit a copy of its information security policy for approval by the Firm’s Security Team.
* **Information Handling At Contract Termination** – Upon the Firm’s termination of its contract with any Vendor organization that is handling Firm information, this same Vendor organization must immediately thereafter destroy or return all of the Firm’s information in its possession.
* **Vendor Information Disposal** - If the Vendor destroys the information, the Firm must receive notice that the data was disposed of properly, and be provided certified proof.

# 9.0 Related Policies

* Account Management
* Information Classification

# 10.0 Related Form

* Vendor Management Due Diligence Checklist

# 11.0 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 |  |  |  |
|  |  |  |  |  |