[Company Name]

Third-party Management

Policy and Procedures Template

# PURPOSE

[Company Name] must assess the risks posed by both its current and potential third-party service providers. It is critical that [Company Name]’s third-party service providers implement controls to identify and remediate deficiencies and/or vulnerabilities on an ongoing basis, in order to ensure the continued effectiveness of security controls to protect [Company Name]’s client confidential data. [Company Name] must ensure the appropriate levels of due care and due diligence are applied to validate that appropriate security controls are in place and implemented correctly.

# RESPONSIBLE INDIVIDUALS

[Company Name] management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the:

* [Company Name] Information Security Officer or his/her designee
* [Company Name] Privacy Officer or his/her designee

# SCOPE

This policy and procedures apply to all Management and workforce members who are responsible for, use or administer [Company Name] information systems that store, process or transmit client confidential data.

# APPLICABLE STANDARDS & DEFINITIONS

The Applicable Standards are based on the control Framework(s) applied.

# ACRONYMS & DEFINITIONS

* **Information Systems**: Any computing resources, software, and data required that perform processing on behalf of [Company Name] clients.
* **Client Confidential Data**: Electronic data provided by a [Company Name] clients that contains PII, PHI, ePHI or other data contractually identified as being Client Confidential.
* **PII**: Personally Identifiable Information.
* **PHI**: Protected Health Information
* **ePHI**: Electronic Protected Health Information as defined by HIPAA.
* **Workforce Member**: Any [Company Name] employee, consultant, contractor or partner who does work on behalf of [Company Name].
* **Significant Change**: A change that is likely to affect the security state of the information system.
* **Third-Party Service provider**: Vendor, Contractor, Business Associates, Managed Service Provider (MSP), Cloud service provider (CSP), Internet Service Providers (ISP) and other entities contracted by [Company Name]

# DISTRIBUTION

The baseline document resides in [[Designated Security Platform] URL]

# POLICY

 [Company Name] should follow a clearly documented process when selecting a third-party service provider. The level of due diligence required will vary depending on the sensitivity of data being handled and the potential impact on overall operations.

 Any third-party service provider that has access to [Company Name] client confidential data must demonstrate they have the capability to protect [Company Name]’s client confidential data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk.

 [Company Name] shall address liability, service definitions, security controls, and other aspects of services management within SLAs or contracts.

 [Company Name] shall maintain a central list of all third-party service providers, particularly those that have access to sensitive data or impact operations. Each third-party service provider should be assigned a risk designation and a designated third-party service provider Owner within [Company Name].

 Third-party service provider owners shall:

* maintain written agreements with each third-party service provider that includes an acknowledgment that the third-party service provider is responsible for the security of client confidential data the third-party service provider possess or otherwise stores, processes or transmits on behalf of [Company Name] or to the extent that they could impact the security of [Company Name];
* conduct, review and document, at least annually, a background check on each critical third-party service provider to ensure they are financially viable and in good standing
* have the third-party service provider complete a security questionnaire
* define and document [Company Name] oversight responsibilities for security control compliance and performance; and
* perform, at least annually, third-party service provider audits/reviews of critical third-party service providers to ensure the third-party service provider relationship is current, properly defined, security compliance is maintained and operating within required SLAs.

 Third-party service providers who use subcontractors to conduct [Company Name] services must have in place a third-party service provider management policy at least equivalent to this one to ensure they are managing their third-party service providers in an equivalent manner.

 Third-party service providers should immediately report any non-compliance such as data breaches or SLA failures to the third-party service provider owner, who in turn should report this to the Designated Security Officer.

**Business Associate Agreements**

Business Associate Agreements (BAs) and other arrangements should specify:

* All client confidential data will be held in strict confidence and accessed only for the explicit business purpose of the contract;
* The service provider must be compliant with and maintain compliance with the protective conditions outlined in the contract;
* The service provider is liable to protect all client confidential data it stores and / or accesses;
* In the event of a security breach, due to its actions or inactions, the service provider shall bear all responsibility and expenses associated with the response to the security breach;
* The service provider must return or destroy all sensitive data received from [Company Name], upon completion of the contract;
* Any violation of the service provider’s security posture amounts to a material breach of contract and entitles [Company Name] to immediately terminate the contract without penalty;
* Auditing of the service provider’s contract performance, security posture and compliance is authorized at any time; and
* The contract’s protective requirements shall survive any termination agreement.

Business Associates, following the discovery of a breach of unsecured PHI must notify [Company Name] of the breach.

The Business Associate will provide to [Company Name] notification of the breach in a timely manner but in no less than 60 days of the first day the Business Associate became aware of the breach.

# PROCEDURES

**Procedure 1**

Third-Party Review & Approval

**Frequency:** As needed, Annually

**Responsible Roles:** [Asset Owner], [Designated Security Officer], [Executive Management]

**Procedure Steps:**

1. Maintain a comprehensive third-party list in [security platform]:
	1. Distinguish critical and non-critical vendors;
	2. Upload all contractual documents, including Business Associate Agreement (BAAs), Non-Disclosure Agreements (NDAs), Service Level Agreements (SLAs), SOC II, as applicable to the terms and conditions of the engagement
2. Review third-party’s contractual documents for compliance. If they do not comply:
	1. Identify and document the deficiencies and risk(s) ;
	2. Take corrective action as necessary.
3. Review third-party’s performance to determine if they are meeting contractual requirements. If they do not comply:
	1. Identify and document the deficiencies and risk(s) ;
	2. Take corrective action as necessary.
4. Review third-party’s security and / or privacy compliance. Ensure [Company Names]'s client confidential data is protected with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk in accordance with the policy requirements. If they do not comply:
	1. Identify and document the deficiencies and risk(s) ;
	2. Take corrective action as necessary.
5. Communicate results of the review with all applicable stakeholders.
6. Document and retain evidence of this review in [Designated Security Platform] with any necessary attachments.

**Procedure 2**

Ensure third-party contracts and agreements address confidentiality as part of the non disclosure terms.

**Frequency**: As necessary, prior to executing any new agreement

**Responsible Roles**: [Asset Owner], [Designated Security Officer], [Executive Management]

**Procedure Steps**:

1. Review proposed contract/service agreement to determine if confidentiality has been addressed as part of the non disclosure terms (or in another area of the agreement).
	1. If it has not, negotiate changes as necessary prior to executing the agreement.
2. Document and retain evidence of this review in [Designated Security Platform] with any necessary attachments.

**Procedure 3**

Ensure third-party contracts and agreements address requirements

**Frequency**: As necessary, prior to executing any new agreement

**Responsible Roles**: [Asset Owner], [Designated Security Officer], [Executive Management]

**Procedure Steps**:

1. Review proposed contract/service agreement to determine if specific requirements have been addressed that include the following as applicable to the engagement:
	1. Scope of services
	2. Product specifications
	3. Roles and responsibilities
	4. Compliance requirements
	5. Service levels
	6. Communications and issue resolution
	7. Termination procedures
2. If they do not, negotiate changes as necessary prior to executing the agreement.
3. Communicate results of the review with all applicable stakeholders.
4. Document and retain evidence of this review in [Designated Security Platform] with any necessary attachments.

**Procedure 4**

Review third-parties performance and assess risk.

**Frequency:** As necessary, at least annually

**Performed by**: [Chief Operating Officer (or their designee)],[Business Operations],[Executive Management]

**Procedure Steps:**

1. Review the third-parties performance to determine if they are meeting the requirements and compliance terms of the agreement.
	1. If they do not:
		1. Identify and document the deficiencies and risk(s)
		2. Take corrective action as necessary.
2. Document and retain evidence of this review.

# COMPLIANCE & ENFORCEMENT

All applicable managers and supervisors are responsible for enforcing the provisions of this document. Workforce members who violate these policies and procedures may be subject to discipline up to and including termination.

# VERSION HISTORY

All document version history resides in [Designated Security Platform]. It includes the following details:

* Version Number
* Document Owner
* Approval
* Origination date
* Updates and description of changes

--

Have questions about this template or need help with your third party risk management program?
[**Get in touch with us!**](https://www.ostendio.com/contact-us)