|  |  |  |
| --- | --- | --- |
| **Policy Title:** | **Third Party Service Provider Policy** | **ID:POL 012** |
| Issued By: |  |
| Policy Owner: |  |
| Last Updated: |  |

This is a sample policy that may be of interest to small businesses in the financial services and insurance industries. It is intended solely for general informational purposes and does not constitute legal advice. Any cybersecurity policy created by a business should be tailored to the business’s specific needs, risks, and resources. The specific circumstances of each business may require actions and procedures beyond those outlined in this sample; likewise, not every action or procedure in this sample will necessarily be appropriate for a particular business. Therefore, a policy based only on this sample may not be fully compliant with any state or federal law or regulation, including DFS’s Cybersecurity Regulation (23 NYCRR Part 500), as each business must both draft policies tailored to its own circumstances and implement those policies effectively. Note that best practices can change quickly in the cyber landscape and what constitutes best practices evolves over time. Businesses should periodically review their policies and update them as necessary. Businesses that are subject to DFS’s Cybersecurity Regulation should also note that the business reflected in the sample is exempt from some requirements pursuant to 23 NYCRR 500.19(a), including the requirement to have a Chief Information Security Officer. Your business may not be so exempted.

# Purpose of Policy

This Policy shall establish requirements by which [ORG] will manage security risks associated with Third Party Service Providers (TPSPs) and all other contracted provider arrangements. The intent is to ensure that the security of [ORG]information and information assets are not reduced when exchanging information with third parties or by the introduction of third party products or services into the [ORG] environment.

# Policy Scope

This Policy covers all [ORG] TPSPs and all other contracted provider arrangements. All [ORG] employees, including third parties and contractors, are required to comply with this Policy.

# Policy Statement

## Risk Management

[ORG] shall manage and address the security risk of TPSPs that may have access to [ORG]’s data or provide products or services to [ORG].

**Objectives**

* + [ORG] will establish a Risk Assessment process to identify, measure, mitigate, and monitor risks to [ORG]’s data, information systems, and Nonpublic Information (NPI) accessible to, or held by, third parties.
	+ [ORG] will establish a due diligence process for prospective TPSPs, which addresses, at a minimum, a TPSP’s:
		- financial condition,
		- reputation,
		- cybersecurity practices,
		- insurance coverage,
		- critical third parties, and
		- strategic partners.
	+ [ORG] will perform a periodic review of adherence to Service Level Agreements (SLAs), cybersecurity measures, and contractual and regulatory requirements.
	+ [ORG] will maintain a current and accurate listing of all TPSPs and conduct a Risk Assessment of each one periodically.
	+ The Senior Officer of [ORG] responsible for [ORG]’s cybersecurity will inform senior management, and the Board of Directors if one exists, of the risks associated with outsourcing agreements to ensure effective risk management practices.

Third Party Risk Assessment

* + [ORG] will establish a checklist or questionnaire to identify the risks of using a TPSP to determine if such third party’s practices could have a negative impact on [ORG]. Elements of a TPSP questionnaire should include the TPSP’s:
		- Need to access NPI, Personally Identifiable Information (PII), or Electronic Health Information (ePHI)
		- Need to access financial or confidential data
		- Need to access [ORG]’s internal network
		- Audit program or SSAE18 report
		- Cybersecurity Program
		- Vulnerability and penetration testing program
		- Cybersecurity insurance or other related insurance
		- Involvement in any recent cyberattack or data breach
		- Compliance with federal and state laws and regulations
	+ [ORG] will review the checklist or questionnaire to evaluate and mitigate risks if possible and to decide whether to pursue the relationship with the third party.
	+ [ORG] will conduct further due diligence to analyze whether the TPSP meets [ORG]’s needs and regulatory requirements.

Third Party Review

* + [ORG] will have a review program to ensure TPSPs are delivering the quantity and quality of services expected and/or agreed upon.
	+ [ORG] will monitor the key aspects of its relationships with third parties, including the security controls and financial strength of each third party, and the impact of any external events on its relationships with third parties.

Third Party Tracking

* + To increase monitoring effectiveness, [ORG] periodically will rank TPSP relationships according to risk to determine which service providers require closer monitoring.
	+ [ORG] will base its rankings on the relationship’s residual risk after analyzing the quantity of risk relative to the controls over those risks.
	+ Relationships with third parties that [ORG] has determined to be higher risk will receive more frequent and stringent monitoring of their performance (financial and/or operational), and more frequent independent control validation reviews.

Third Party Service Reporting

* + [ORG] will monitor the service, reports, audits, and records provided by a TPSP and review them at intervals that will be based on their risk ranking.
	+ [ORG] will conduct independent audits to ensure TPSPs are complying with their agreements and all requisite laws and regulations.
	+ [ORG] will conduct regular meetings as required by SLAs and TPSP agreements to review reports, audit trails, security events, operational issues, failures, and disruptions, and will investigate and resolve identified issues.
	+ [ORG] periodically will audit network connections with TPSPs to ensure that the connections are appropriate and meet all agreed upon requirements.

# Policy Approval

[ORG] will review this Policy periodically for accuracy, completeness, and applicability, and will revise and approve it annually.

# Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **DFS’s Cybersecurity Regulation** | A set of regulations promulgated and enforced by the New York Department of Financial Services (DFS) regarding cybersecurity. The regulations can be found in Part 500 of Title 23 of New York Codes, Rules and Regulations (NYCRR).  |
| **Electronic Protected Health Information (ePHI)** | Individually identifiable health information, including demographic information collected from an individual, that is protected by federal law pursuant to the Health Insurance Portability and Accountability Act, and related laws and regulations, and is transmitted by, or maintained in, electronic media. ePHI includes information that identifies an individual or might reasonably be used to identify an individual and relates to: an individual’s past, present or future physical or mental health or condition; the provision of health care to an individual; or the past, present or future payment for health care to an individual. Individually identifiable health information includes, but is not limited to, many common identifiers (e.g., name, address, birth date, Social Security Number). *See* 45 C.F.R. 160.103. |
| **Multifactor Authentication (MFA)** | An electronic authentication method in which a user is granted access to a website or application only after successfully presenting to an authentication mechanism two or more pieces of evidence which could be something the user and only the user knows, something the user and only the user has, or something the user and only the user is. |
| **Nonpublic Information (NPI)** | All electronic information that is not publicly available information such as business-related information which unauthorized disclosure, access or use of which would cause a material adverse impact to the operations or security of the business. A combination of any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual. Any health care information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual. |
| **Personally Identifiable Information****(PII)** | Any data that is not available to the general public and that could be potentially used to identify a particular person. Examples include full name, mailing address, email address, Social Security number, driver’s license number, bank account number, and passport number. |
| **Penetration Testing Program** | The practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. The main objective of penetration testing is to identify security weaknesses, report those weaknesses to management, and remediate the weaknesses in a systematic way. |
| **Risk Assessment** | A risk assessment is the combined effort of: identifying and analyzing potential events that may negatively impact an organization’s assets, and/or the environment; making judgments based on the likelihood and impact of the negative events; and addressing those events in a systematic way. |
| **Senior Officer** | A senior member of [ORG] who is responsible for the oversight and implementation of [ORG]’s Cybersecurity Program or for the direction and oversight of a Third Party Service Provider hired by an organization to be responsible for implementing its Cybersecurity Program. A Senior Officer can also be the Chief Information Security Officer. |
| **Service Level Agreement (SLA)** | A commitment between a service provider and a client that covers services to be provided and highlights the quality standards that are required of the provider to guarantee client satisfaction. |
| **SSAE 18** | Statement on Standards for Attestation Engagements No. 18, produced and published by the American Institute of Certified Public Accountants Auditing Standards Board.  |
| **Third Party Service Provider (TPSP)** | A person or entity that provides services and maintains, processes or otherwise is permitted access to an organization’s Nonpublic Information through its provision of services to that organization. A third party is not an affiliate of [ORG]. |
| **Vulnerability Management** | The systematic practice of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities. |

# Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Title** | **Description** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |