Wishes Vendor Management Policy

INTRODUCTION

The purpose of this policy is to establish a framework for management of third-party agreements, controls and objectives that support Wishes business needs and requirements. This document may be revised by Vendor Management as necessary and submitted to Senior Management for approval.

As a small company there is not a dedicated person but assumed and managed by our Ceo Annie Rhodes. She is the owner of this document and is responsible for ensuring proper policies, procedures and standards are developed that will apply to Wishes and employees involved in the management of third-party service providers. The Vendor Management Program focuses on these five (5) distinct topics:

- Governance
- Roles and Responsibilities
- Contract Administration
- Processes and Controls
- Vendor Assessment, Monitoring and Performance Evaluation

GOVERNANCE

The Board of Directors delegates to Wishes management the authority to implement operational policies and procedures to address the entire lifecycle of third-party vendor management. Wishes management will establish procedures to implement this policy and all revisions, modifications and amendments to procedures will be subject to its approval.

DEFINITIONS

The following definitions are provided for the purpose of clarity throughout this policy:

Vendor: Third-party service provider, either a company or an individual, that provides a product or performs a service for Wishes and meets any of the following criteria:

- Performs services at Wishes facilities (safety, insurance or data security risk)
- Has access to customer or other sensitive data (data security risk)
- Has a contractual commitment to Wishes (financial or customer service risk)

Contract or Agreement: A legal document, between Wishes and a third-party vendor, in which the vendor agrees to provide services or products, and for which Wishes agrees to render payment.

Vendor Risk Rating: A Low, Medium, or High rating assigned because of the "Vendor Risk Assessment" that indicates the relative risk this vendor represents to Wishes

ROLES AND RESPONSIBILITIES

Vendor Management Officer's Role

Wishes management assigns oversight and management of all Vendor Management Program activities to the Vendor Management Officer. The Vendor Management Officer's role includes providing guidance and direction on sourcing and vendor management practices to Wishes employees. The Vendor Management Officer also manages compliance with the vendor due diligence process for vendor selection and monitoring.

The Vendor Management Officer may assign certain management and negotiation responsibility to a relationship manager within the business, as appropriate, but is responsible for maintaining oversight in those instances.

The Vendor Management Officer is responsible for developing, implementing and maintaining policies, processes and procedures to maximize the benefits to Wishes and mitigating third-party risks associated with outsourcing services.

The basic duties of the Vendor Management Officer include, but are not limited to, the following:

- Defining and implementing the Vendor Management Policy and Procedures
- Defining and administering process requirements and internal controls for engaging vendors
- Maintaining the inventory of third-party service providers, including:
    - Name of third-party service provider
    - Date of contract
    - Date of contract expiration
    - Minimum review cycle based on risk assessment
- Contract administration/management/negotiations:
    - Administration of the contract life cycle
    - Standardization of Wishes contract business terms

    - Ensuring applicable contracts include the requirements to provide Wishes the necessary due diligence information as related to confidentiality and security of customer data
    - Managing contract record keeping
    - Coordination with the business to conduct strategic relationship reviews
    - Negotiating contract terms and pricing
- Obtaining due diligence documentation from third-party service providers when necessary
- Collaborating with internal business leaders to obtain due diligence documentation from third parties. These could include, but are not limited to:
    - Information Security Policy
    - SOC Reports
    - Financial Statements
    - E&O Policies
- Monitoring vendor compliance and performance:
    - Ensuring vendors meet contract terms including service level agreements (SLA's) as well as adhere to applicable state and federal guidelines
    - Ensuring third-party relationship managers within the business follow the prescribed due diligence program
    - Facilitating annual contract compliance and risk assessment reviews for critical third-party relationships
- Training and Communication:
    - Educating business relationship managers about policies and best practices (e.g. vendor lifecycle management and contract negotiations)
    - Fostering adherence to existing policies and procedures
    - Communicating and training business relationship managers on the vendor management requirements of this policy.
    - Maintaining training records and content
- Establishing risk-based Information Security diligence requirements of the third-party service provider
    - Due diligence checklist
    - Onsite visit requirements for critical vendors
    - Organizing third-party onsite visits to Wishes facilities
    - Scheduling and conducting onsite visits of third-party
    - Documenting onsite visit results
    - Scheduling and completing any subsequent site visits and diligence
    - Reporting on findings and recommendations for ongoing relationship with third-party

Business Unit Relationship Manager Responsibilities

To the extent the Vendor Management Officer is not already engaged, the Business Unit Relationship Manager is responsible for the following:

- Engaging the Vendor Management Officer on all contract related matters to ensure contract negotiations and contract terms meet Wishes standards
- Engaging Legal, when applicable, to review contracts prior to execution
- Reviewing contracts to ensure billable services were performed as indicated
- Ensuring invoices are received and submitted in a timely manner to Accounts Payable for payment

- Monitoring the third-party service provider for adherence to service level commitments and project milestones
- Ensuring regular reporting from vendors are provided, when applicable
- Conducting periodic risk reviews of vendors risk reviews of vendors to ensure vendor performance remains within Wishes established risk appetite

CONTRACT ADMINISTRATION

Standardized Terms and Conditions

The Vendor Management Officer is responsible, in conjunction with Legal, for determining the contract terms and conditions to be used for all contractual obligations. The Vendor Management Officer is responsible for documenting and implementing these standards.

Contracts between Wishes and prospective third-party service providers should consider business requirements and key risk factors identified during the risk assessment and due diligence phases. Contracts should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality and reporting.

Management should consider whether the contract is flexible enough to allow for changes in technology and Wishes operations.

Appropriate legal counsel should review contracts prior to signing. Legal review of the proposed contract may be performed by internal or external counsel with sufficient knowledge of Wishes business and operations. Wishes should always engage external counsel to review contracts for high-risk vendors or those with significant impact on business operations or if trademark or intellectual property rights are at risk.

Contract Negotiations and Requirements

A formal contract with a third-party service provider will be required as determined by the Vendor Management Officer. Generally, all contracts must include the standards established by the Vendor Management Officer. Exceptions to this policy can be approved by the Vendor Management Officer, Legal, or the Chief Executive Officer, or his designee.

Contract language should be reviewed to ensure that the agreement or contract meets regulatory requirements and does not expose Wishes to unnecessary risk.

Cancellation of a contract must follow agreed upon contract language and be executed at the same or higher level of the organization as the original contract execution. Contract cancellation must be completed in writing.

Document Archiving and Record Retention

The Vendor Management Officer is responsible for storing and securing signed contracts and ancillary documents. Vendor contract files will be stored for four years after contract expiration in compliance with California Civil Code that identifies the statute of limitations for California contracts as four years.

Contract Requirements, Review and Approvals

The CEO will determine allowable signing authority on contracts until such time a formal Accounts Payable Signing Authority Policy is set for the firm.

PROCESS AND CONTROLS

Defining Business Objectives

Prior to vendor selection, clearly defined business objectives and requirements are crucial for deciding if an internal or external solution is the desired course of action. These definitions will also help scope the pre-bid statement of work and the depth of risk assessment required. This initial stage is led by the CEO to evaluate alternative solutions and prospective vendors. The following should be performed:

- Business objectives to be achieved through new acquisition or partnership
- Consulting with affected business units and other stakeholders
- Foreseeing and determining the criticality of the system or service to the organization
- Defining general criteria to determine if the scoping goals have been met.

Risk Assessment

Prior to a new contract or renewing an existing contract for a business product or service, the Relationship Manager is responsible for submitting a written assessment to the Vendor Management Officer, which includes:

- Purpose of vendor/contract and/or service provided
- Expected annual cost of the vendor
- Name and contact information of vendor
- Any additional relevant information

The Vendor Management Officer will complete a risk assessment to determine whether the vendor is a High, Medium, or Low risk vendor.

Prior to selection of a business product or service, the Business Unit Relationship Manager must contact the Vendor Management Officer to discuss the scope of risk.

The risk assessment will consider the impact to the following:

- Strategic goals, objective and business needs
- Importance and criticality of the services to Givewishy
- Contractual obligations and requirements of the vendor
- Threats to information technology and physical security
- Confidentiality of Wishes business confidential or sensitive information
- Financial condition of the vendor
- Reputation risks

- Operational risks
- Compliance exposure

For Medium and High-Risk vendors, the Vendor Management Officer will also determine the adequacy of the vendor's standards, policies and procedures relating to internal controls including but not limited to regulatory compliance, privacy protections and business continuity plans and assess the adequacy of the vendor's insurance coverage.

The Vendor Management Officer must complete a risk assessment prior to the engagement of the third-party service provider. The **Vendor Risk Assessment Template** is attached as **Appendix A.**

The risk assessment template cannot fully represent a vendor's risk to Wishes and ultimately the Vendor Management Officer must determine the level of risk. For example, despite their importance to the company, especially large vendors such as Google, Hetzner and Github are relatively lower risk given their size, widespread usage and investment in technology.

Based on the results of the risk assessment, the Vendor Management Officer will determine the level of due diligence required.

Risk assessments should be revisited as part of the contract renewal or anytime the relationship with the vendor changes in a significant way.

Due Diligence

Relationship Managers are responsible for identifying and evaluating potential vendors prior to selection for a business product or service, as follows:

- Assess the vendor's experience and ability to provide the necessary services for current and anticipated needs of Wishes
- Evaluate the vendor's reliance on third parties or partners that would be used to support the outsourced operations and determine if a separate agreement and risk assessment is required for the 4th party vendor
- Evaluate the experience of the vendor in providing services in the anticipated operating environment
- Evaluate the vendor's ability to respond to service disruptions
- Evaluate the adequacy of resources assigned to meet Wishes anticipated business activity supported by the vendor
- Perform on-site visits, where necessary, to better understand the vendor's operations.

Medium and high-risk vendors must also complete a due diligence questionnaire to be returned to the Vendor Management Officer for review. The **Due Diligence Questionnaire** is included in **Appendix B.**

The Due Diligence Questionnaire is primarily aimed at vendors who provide financial services but can be adapted based on the specific vendor.

High Risk Vendors

In addition to the risk assessment and due diligence detailed above, for high-risk vendors, Business Unit Relationship Managers are responsible for staying abreast of the vendor's

financial condition on at least an annual basis by reviewing audited financial statements, if available.

The evaluation should include the following:

- Consideration of the significance of Wishes proposed contract on the vendor's financial condition.
- Evaluation of technological expenditures, such as vendor's level of investment in technology consistent with supporting Wishes activities and the vendor's financial resources available to invest in and support the required technology.

VENDOR ONGOING MONITORING AND PERFORMANCE

Vendor Oversight

An oversight program monitors critical vendor controls, condition and performance. Significant events at the vendor level may affect Wishes outsourcing relationship. Such events may include business changes such as acquisition, organizational shifts or changes in volume or technology changes such as application and operating system upgrades, hardware changes and other changes in the technology environment.

The responsibility for monitoring vendor condition and performance is assigned to the Business Unit Relationship Manager with oversight by the Vendor Management Officer.

Monitor Financial Conditions and Operations

Relationship Managers are responsible to monitor its vendor's financial condition and operations at least annually for high-risk vendors. Documentation of the review is required to meet compliance requirements. The Relationship Manager must:

- Periodically, not less often than annually, review the vendor's policies relating to internal controls by obtaining a SOC 2 report, when available, and ensure they are consistent with the current market and technological environment
- Monitor changes in key vendor project personnel allocated to Wishes
- Review and monitor the vendor's insurance policies for effective coverage

Assess Quality of Service and Support

Relationship Managers are responsible to evaluate, document and report vendor performance against service levels agreed upon on at least a semi-annual basis. Any issues with services levels will not be held until the review, rather will be addressed immediately to improve performance or replace the third-party service provider. The Business Unit Relationship Manager must:

- Document and follow up in a timely manner on any service delivery issues
- Evaluate the vendor's ability to support Wishes business
- Review consumer complaints on the products and services provided by the vendor
- Periodically (at least annually for high risk/high touch third parties) meet with the vendor to discuss performance, resources and operational issues.

Monitor Contract Compliance and Revision Needs

Relationship Managers are responsible to conduct a review of its vendor obligations per the contract agreement on at least an annual basis for high-risk vendors.

- Review the contract for the following events: scheduled risk assessments, scheduled performance reviews, scheduled financial reviews, contract reviews, contracts due for renewal and contract expirations;
- Review invoices to ensure proper charges for services rendered;
- Review the vendor's performance relative to service level agreements; and
- Review the vendor's disaster recovery plan and business continuity plan to ensure any services considered critical for Wishes can be restored within an acceptable time frame.

VERSION CONTROL

Version 1.1 Oct 2022

Appendix A: Vendor Risk Assessment

Vendor Risk Assessment Matrix				
Criteria	Low	Medium	High	Point Attribute
	1 point	2 points	3 points	
Business impact/ Operational Risk [What is the potential business impact on Givewishy if the vendor fails to perform?]	Minimal [Disruption of service would cause minimal impact to business operations]	Significant, but non-critical [Disruption of service may cause some impact to business operations]	Critical [Disruption of service would cause impact that would be critical to business operations]	
Customer Contact [How much customer contact does the vendor have?]	None	Indirect	Direct	
Level of Wishes provided NPI [What is the level of non-public information provided to the vendor?]	None	Name and address	Name, address, and other PII PII is defined as information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Samples of PII include email address, driver's license, telephone number, date of birth.	

Information Security [How much access does vendor have to Wishes systems, servers or confidential information?]	Minimal access to Wishes systems, servers or confidential information.	Moderate access to some systems, servers or confidential information.	Integration with or full access to Wishes systems, servers or confidential information.	
Regulatory Exposure [How much regulatory compliance is required for this specific vendor]	Minimal regulatory compliance required	Some regulatory compliance required	Significant regulatory compliance required	
Replacement Difficulty [How difficult will it be to replace this vendor with another vendor]	Many substitutes, requires little time to replace	Few substitutes, requires some time to replace	Difficult to find substitute, requires significant amount of time to replace	
Reputational Risk [What is the reputational risk to Wishes if the vendor fails to perform?]	Little impact on business reputation	Some impact on business reputation	Significant impact on business reputation	
Vendor Industry Exposure	Large, well-known vendor / public company (Hetzner)	Developed policies and procedures, moderately well known in market. (Slack)	Newer vendor in the market, limited experience, in early growth stage.	
Expected Annual Spending	<$25,000	$25,001-$50,000	>$50,000	

Point Total*				

***The point total may be overridden for services that are provided by large, nationwide service providers, such as Hetzner, Github, Slack, etc.**

Risk tier ratings are assigned to each vendor based upon a total risk score calculated pursuant to the Vendor Risk Assessment.

Tier	Risk Level	Risk Score	Definition
Tier 1	Low Risk	<3 points	Represents low risk to Wishes, requires low oversight
Tier 2	Medium Risk	<6 points	Represents medium risk to Wishes requires moderate oversight;
Tier 3	High Risk	>10 points	Represents significant risk to Wishes and requires continuous oversight such as annual due diligence review