Vendor Management Policy

Version number	3.2
Last Approved	Apr 24, 2025
Classification	PUBLIC

Overview

This Vendor Management Policy establishes criteria for adoption and qualification of new vendors, evaluation of vendor performance and compliance, risk identification and mitigation, and termination of a vendor relationship.

Applicability

The applicability of this statement falls under purview of the Security Documentation Overview.

Purpose

This policy ensures the Company performs its due diligence in regards to assessing vendor risk and performance to ensure the security and privacy of Company and customer data.

Scope

This policy applies to vendors providing information services within the scope of the Company’s development and hosting of client-facing services, as well as it’s internal operations.

Vendor Management Policy

New Vendor Due Diligence

Prior to onboarding new vendors, the Company must perform due diligence to ensure that engaging the vendor does not pose unreasonable risk to the Company or its customers. The Company shall ensure that the third party’s security commitments are at least as rigorous as the Company’s.

SOC 2: CC9.2

The entity assesses and manages risks associated with vendors and business partners.

Below are the criteria used to determine the risk classification of each vendor and the due diligence methods required for each classification:

Critical Risk/Sub-processors

Criteria

- Vendors that have access to, store, or process client data or restricted information.
- Sub-processors.
- Vendors that pose the highest risk if data is lost, including breach of contract or regulatory compliance risk.
- Vendors who's downtime could result in failure or inability to deliver services.
- Vendors that pose a high financial risk and may be difficult to replace.
- Vendors embedded into core networks, applications, or processes

Process

- Critical risk vendors are considered the highest risk vendors and therefore, undergo a thorough review.
- Applicable SOC reports and Certifications need to be reviewed and verified.
    - Review SOC 1 Type 1 for Financial Tools and PCI compliance for payment processors. SOC 2 Type 2 for all others.
    - Supplemental documentation may be acceptable (ISO Certification, HIPAA compliance, security questionnaire, security page, penetration test report, risk assessment reports, etc.).
    - Exceptions in compliance reports are reviewed for potential risk to the Company.
- Any recent security breaches and lawsuits are notated and reviewed.
- Applicable service agreements / terms of service are reviewed.
- Acceptable Data Processing Addendum and/or Security Addendum is obtained.

High Risk

Criteria

- Vendors that process confidential data supporting sensitive or core processes.
- Vendors on which the Company is highly dependent on operationally.
- Vendors who's downtime could result in significant but not critical disruption to the Company.
- Vendors that pose a medium financial risk and may be hard to replace.

Process

High risk vendors undergo a vetting process substantially similar to critical vendors but with a slightly less rigorous expectations.

Medium Risk

Criteria

- Vendors that process internal or confidential data supporting auxiliary processes.
- Vendors who’s loss of service does not cause significant disruption.
- Vendors that are easily replaceable.

Process

- Medium risk vendors undergo a vetting process which entails the review of available documentation related to the vendor’s security, stability, and privacy capabilities, etc.
- While there are no specific certification or documentation requirements, the review must ensure there is adequate information available to effectively assess the vendor’s capabilities.

Low Risk

Criteria

- Vendors that only process public or internal non-sensitive data.
- Vendors who’s loss of service does not pose any substantive disruption to the business.
- Vendors that can be easily replaceable.

Process

- Low risk vendors undergo a vetting process substantially similar to medium risk vendors but with slightly more flexibility.

Review Cadence

All vendors must be reviewed prior to onboarding and annually thereafter. Vendors onboarded less than 9 months from the annual review are exempt from reevaluation. If the nature or scope of the services provided or the use cases for how the service is consumed by the Company change materially, the vendor must undergo additional review.

The GRC Team also conducts monthly reviews to monitor the overall performance of the Vendor Management Process.

All vendor assessments must be retained for at least 5 years.

Offboarding Vendors

Due diligence and risk management must be performed throughout the vendor lifecycle, including when offboarding a vendor. Below are two key considerations to consider whenever a vendor is being offboarded.

Data Deletion

When terminating a relationship with a critical risk vendor, the Company must ensure that the vendor deletes all confidential data retained from the lifetime of the engagement within a reasonable timeframe. Deletion of confidential data stored by the vendor not only protects the Company's sensitive information but also helps achieve the Company's confidentiality commitments to its own customers. Refer to Data Retention, Destruction and Disposal Policy for compliance guidelines.

Preservation of Audit Evidence

When a vendor is offboarded, care must be taken to assess any related data retention requirements. For example, evidence required to support upcoming audits.

Document control

ⓘ This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @angelina.kilmer @Paul Gordon	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Feb 25, 2025
Review cycle	ANNUAL	
Next review date	Feb 24, 2025	

Version History

Date	Author(s)	Version	Changes
May 14, 2025	@angelina.kilmer @Paul Gordon	3.2	Clarification on vendor assessment retention period
Apr 24, 2025	@Paul Gordon @angelina.kilmer	3.1	Updated vendor risk/process details, & cadence section.
Feb 25, 2025	@Art Machado @angelina.kilmer @Paul Gordon	3.0	Annual review
Nov 1, 2024	@angelina.kilmer	2.2	Changed Policy classification from Confidential to Public
Mar 13, 2024	@Art Machado , Sarah Zwicker, @Paul Gordon	2.1	Annual review
Oct 26, 2023	@angelina.kilmer , Sarah Zwicker	2.0	Updated Vendor Risk criteria/process as it relates to due diligence
Sep 21, 2023	Sarah Zwicker & @John Cole	1.7	Format updated, moved to Global Policy Register
Aug 3, 2023	Sarah Zwicker & @John Cole	1.6	Updated scope to include employee PII, revised offboarding and added link to procedure.

Feb 23, 2023	Sarah Zwicker & @Art Machado	1.5	Annual review + logo change
Mar 24, 2022	Sarah Zwicker	1.4	Added Privacy considerations and components
Mar 16, 2022	Sarah Zwicker & @Art Machado	1.3	Title change for VP InfoSec, Annual Review
May 25, 2021	Sarah Zwicker & @Art Machado	1.2	Pulled out procedure elements and created new Vendor Management Procedure.
Mar 11, 2021	Sarah Zwicker	1.1	Changed formatting, added Document Control, Change log, confidentiality statement and added references to LTG.
Feb 24, 2021	@Art Machado	1.0	Original version