INSTRUCTIONS

Third-Party Risk Management Policy Template

Based on regulatory guidance

Venminder's complimentary template can assist you in developing a comprehensive policy that reflects common regulatory expectations and best practices. The template can also help you identify the correct structure and flow of a well-written Third-Party/Vendor Risk Management Policy.

If you're new to writing policies or need a refresher, we strongly recommend you review Venminder's companion document, **"Third-Party/Vendor Risk Management Policy Guidelines: Based on regulatory guidance"**.

Download a copy of the **"Third-Party/Vendor Risk Management Policy Guidelines: Based on regulatory guidance"**

NOTE:

- While this policy template has been created to reflect current regulations and best practices, Venminder makes no warrants or representations regarding the content provided. Your organization is solely responsible for its third-party or vendor risk management policy's structure, content, and regulatory compliance.

- It's your responsibility to adjust, review, and confirm the content to ensure that it accurately reflects your organization's governance structure, requirements, rules, terminology, processes, etc.

Customizing the Template

Approach: Venminder makes no representation that there is a single "one-size-fits-all" approach to third-party risk management. However, this document describes a fully functioning third-party risk management process, including thoroughly examining active and prospective third parties.

Regulatory guidance: The policy template reflects general regulatory guidance and best practices. If you're regulated, make sure you list what regulations your organization observes in the policy. (See Section 2, Statement of Purpose)

Policy vs Program: As a policy is meant to detail what must be done, we have intentionally limited the narrative regarding how it shall be done. This type of detail should not be included in a policy document but rather in a formal program and/or procedure document. We recommend that your organization create program and procedure documents to accompany your policy. You can read Venminder's "Developing Your Third-Party Risk Management Program Document Checklist" for more information on creating a program document.

Separation of duty: The separation of duties is intended to prevent unilateral actions from occurring within an organization's workflow or processes, which can lead to damaging events beyond the organization's risk tolerance. In general, no individual or group should have total control over processes that allow them to ignore errors, falsify data, or commit fraud.

Align to actual practices: This document should accurately describe the rules enforced and the work performed. Please review this document carefully and consider whether it accurately portrays the actual practices in place at your organization. If it doesn't, you must modify the document to represent the existing processes or change them to match the policy.

Formal approval: Your completed policy should be carefully reviewed and formally approved by your senior management and board of directors (if required by regulators) before adopting or making it effective.

Keep your policy up to date: As there are material changes to your processes, regulations, or framework, you must review and update the policy accordingly.

When in doubt, leave it out: The policy template reflects regulatory expectations and best practices. But suppose you don't have an internal requirement to complete due diligence before signing the contract. Or your senior management and board don't approve the policy. In that case, it's best to omit the content saying you do. Remember, having a policy representing your current state and

practices is always better. An auditor will not look favorably on an aspirational policy or one that is not enforceable. If you find gaps between your organizational practices and best practices represented in the policy template, make a note and work towards adding the processes and requirements later. Constant improvement is a good goal, but you must start where the organization is and work from there.

Consistency matters: Ensure you are consistent with specific terms throughout the document. Your policy should use the same terminology, risk levels, risk types, etc., in your third-party risk management program. Avoid referring to something one way in the policy and another way in your third-party risk management platform. The terminology used in your platform should harmonize with your policy.

Define critical and risk levels: Ensure you have a written and agreed-upon definition of what conditions make a third party "critical" to your organization. Likewise, spell out specific attributes of each risk level. Remember that your risk rating methodology and definition of critical should be the same in your policy, processes, and any systems of record (third-party risk management software) used. For information on determining criticality, please visit our "Identifying Critical Vendors: 6 Fool-Proof Questions" infographic.

References to your organization: Section 1 highlights an area to reference your company name. You can spell out the full name each time or you can use a short name or general description that allows you to refer to your organization without using the full legal name in every reference throughout the policy. For example, your organization may be called National Gigantic Bank but you only need to spell that out once. After that, it is acceptable to use an acronym such as NGB or even say "the bank." You could also reference the "organization," the "firm," or the "company." Make sure you also pay attention to instances where the short name or description is possessive, such as "the bank's program," "the company's board of directors", or "the firm's employees". Likewise, you need only reference the full name of the policy once and then as "the policy" after that.

Ensure you refer to your Third-Party or Vendor Risk Management program properly: For example, do you call your program Vendor Risk Management or Third-Party Risk Management? Always use the same name to refer to your program and practices. That applies to any acronyms as well, such as TPRM or VRM. Make sure you refer to these consistently throughout the document. The document highlights these references in RED TEXT to help you ensure consistency.

Organizational terminology: Ensure all terminology used within your organization is consistent (individual roles, processes, policy names, department names, etc.). Assume you use names and terminology in your policy that do not align with typical organizational descriptions. As a result, stakeholders might become confused, and auditors might raise an eyebrow. Suppose you refer to Vendor Owner in your policy, but everyone else knows that role as a Product Manager. In that case, your policy might be misunderstood or ignored.

Seek stakeholder review and feedback: Make sure your key stakeholders can review and provide feedback on your policy. They can bring valuable observations and suggestions to the table. And they can also point out where there are possible issues or roadblocks to success.

Make it look good: If your organization has specific format requirements (font, layout, numbering conventions, etc.) for formal documents such as policies, make sure to follow them. Check for grammar and spelling mistakes. Remove colored text and highlights, and have a second set of eyes review the final draft.

Keep it fresh by scheduling a review: After going through the hard work of writing your policy and getting it approved and implemented, make sure you keep it current. Schedule an annual policy review to review and update your policy to reflect material adjustments in your rules, requirements, or regulatory changes. Keep notes of any changes necessary and changes made. Be sure to update the document revision history in the policy document.

See how Venminder can power other aspects of your third-party risk management.

Request a Demo