Third Party Risk Management Policy

Policy Owner

Approved by

Effective Date

Version

Next Review Date

1. Purpose

This Third Party Risk Management Policy establishes the requirements for identifying, assessing, approving, monitoring, and managing risks arising from the Company's relationships with third parties.

The purpose of this Policy is to help (“***Company***”) protect its information, systems, finances, operations, customers, employees, and reputation while engaging third parties that provide goods, services, technology, access, support, or other business value.

2. Scope

This Policy applies to all Company personnel involved in selecting, engaging, managing, renewing, or ending a relationship with a third party.

For purposes of this Policy, a third party includes any vendor, supplier, contractor, consultant, service provider, distributor, agent, business partner, outsourced service provider, or other external organization that provides products or services to the Company or accesses Company resources.

This Policy applies before a third party is engaged and throughout the relationship, including renewal, material changes in services, and termination.

3. Policy Statement

The Company will take a risk-based approach to third-party management. No third party may begin providing services, receive access to Company systems or information, or process Company data until the required review and approval process has been completed.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

The level of review, contractual protection, and ongoing oversight must be appropriate to the nature of the relationship and the risk presented. Higher-risk third parties require more detailed assessment, stronger safeguards, and more frequent monitoring.

4. Definitions

Business Owner means the Company employee or department responsible for requesting, managing, and evaluating a third party relationship.

Confidential Information means non-public information belonging to the Company, its customers, employees, or other protected parties.

Personal Data means information that identifies, relates to, describes, or can reasonably be linked to an individual.

Third Party Risk Assessment means the Company's review of risks associated with a prospective or existing third party.

Material Change means a significant change to a third party's ownership, services, systems, data handling practices, security posture, location of services, subcontracting arrangements, or other circumstance that may affect risk.

5. Roles and Responsibilities

5.1 Business Owners

Business Owners must submit third-party requests before engagement, provide accurate information about the proposed relationship, participate in risk reviews, and remain accountable for monitoring the third party's performance.

Business Owners must promptly notify the appropriate internal teams of any material change, service issue, suspected security incident, or compliance concern involving a third party.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

5.2 Procurement or Vendor Management

[ ] is responsible for maintaining third-party records, coordinating the intake process, confirming required reviews are completed, and supporting contract and renewal management.

5.3 Information Security and Privacy

[ ] and [ ], where applicable, are responsible for reviewing third parties that may access Company systems, Confidential Information, or Personal Data. These teams may require additional safeguards, documentation, remediation, or monitoring based on the assessed risk.

5.4 Legal and Compliance

[ ] and [ ] are responsible for reviewing contractual, regulatory, ethical, sanctions, anti-corruption, and other legal or compliance risks as appropriate.

5.5 Finance

[ ] may review a third party's financial stability, payment terms, insurance, and financial risk when the relationship is material to Company operations or involves significant spending or financial exposure.

5.6 Senior Management

Senior Management or the designated approval authority must approve relationships classified as high risk and any exception to this Policy.

6. Third-Party Intake and Risk Assessment

Before engaging a third party, the Business Owner must provide sufficient information for the Company to assess the proposed relationship. The information should include the third party's identity, ownership information when relevant, description of services, anticipated access to Company resources, types of information involved, service locations, use of subcontractors, contract value, and business criticality.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

The Company will assess the third party using risk factors that may include:

- Access to Company systems, facilities, networks, or accounts
- Access to Confidential Information or Personal Data
- Processing, storage, transmission, or disposal of Company information
- Impact on customers, regulated activities, or essential business operations
- Financial exposure or dependency on the third party
- The third party's cybersecurity, privacy, legal, compliance, and operational practices
- Geographic, reputational, sanctions, fraud, or corruption risks
- Reliance on subcontractors or other downstream providers

The Company may request questionnaires, policies, audit reports, security certifications, financial information, insurance certificates, references, test results, or other evidence necessary to complete the assessment.

7. Risk Classification

Third parties will be classified according to their level of risk.

Risk Level	Description	Required Oversight
Low Risk	The third party has limited business impact and does not access Company systems, Confidential Information, or Personal Data.	Basic business review and documented approval.
Moderate Risk	The third party supports important business activities or may receive limited access to Company information or systems.	Risk assessment, appropriate contractual protections, and periodic review.
Hgih Risk	The third party supports critical operations, has significant access to systems or sensitive information, processes Personal Data, or presents substantial financial, legal, compliance, or reputational risk.	Enhanced due diligence, formal approval, detailed contract controls, remediation of material findings, and ongoing monitoring.

The Company may adjust a risk classification when new information becomes available or the nature of the relationship changes.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

8. Due Diligence Requirements

Due diligence must be completed before the third party is approved, unless an exception is granted under the Exceptions clause.

Due diligence must be proportionate to the assessed risk and may include review of the third party's:

- Business reputation, ownership, and financial stability
- Information security controls and incident response practices
- Privacy and data protection practices
- Regulatory and legal compliance history
- Insurance coverage
- Business continuity and disaster recovery capabilities
- Use and oversight of subcontractors
- Ethical conduct, anti-corruption controls, and conflicts of interest
- Ability to meet contractual service, quality, and performance requirements

If due diligence identifies material concerns, the Company may require remediation before approval, impose additional contractual obligations, limit the third party's access, or decline the engagement.

9. Contractual Requirements

All third-party relationships must be documented in a written agreement or other written instrument approved through the Company's contracting process, unless the relationship is expressly exempted in writing by _____.

The agreement must be appropriate to the third party's risk level and may include provisions covering the scope of services, fees, confidentiality, information security, privacy, service standards, audit or assessment rights, insurance, subcontracting, incident reporting, record retention, intellectual property, compliance with applicable laws, indemnification, limitations of liability, termination rights, and return or secure deletion of Company information.

Where a third party processes Personal Data or Confidential Information, the agreement must require the third party to protect that information using reasonable and appropriate safeguards and to use it only for authorized purposes.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

10. Information Security and Data Protection

Third parties may receive access only to the systems, information, facilities, and resources reasonably necessary to perform their approved services.

Access must be authorized, documented, and reviewed periodically. The Company may require controls such as multi-factor authentication, encryption, access logging, role-based access, secure data transfer methods, and employee background checks where appropriate to the risk.

A third party must promptly notify the Company of any actual or suspected unauthorized access, disclosure, loss, alteration, or unavailability of Company information. The third party must cooperate with the Company in investigating and addressing the incident.

11. Ongoing Monitoring

Business Owners must monitor third-party performance throughout the relationship and confirm that the third party continues to meet contractual, operational, security, and compliance requirements.

The frequency and depth of monitoring will depend on the risk classification. Monitoring may include service reviews, performance reports, updated due diligence materials, security attestations, audit reports, compliance certifications, incident history, financial reviews, and reassessments.

High-risk third parties must be reassessed at least every _____ months, or more frequently if required by the nature of the services or a material change.

12. Material Changes and Risk Events

The Business Owner must notify _____ and the appropriate internal teams before approving or implementing a material change involving a third party.

A third party must be reassessed when there is a material change or risk event, including a significant security incident, change in ownership, financial distress, regulatory investigation, adverse media report, substantial service failure, or expanded access to Company systems or information.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

The Company may suspend access, require corrective action, revise contract terms, or terminate the relationship when a risk event creates an unacceptable level of exposure.

13. Issue Management and Remediation

Identified concerns must be documented and assigned to an accountable owner. The responsible third party and Business Owner must develop and follow a remediation plan when corrective action is required.

Remediation plans must describe the issue, required action, responsible party, target completion date, and method of validation. The Company may escalate overdue, unresolved, or material issues to Senior Management.

14. Termination and Offboarding

When a third-party relationship ends, the Business Owner must coordinate with the appropriate internal teams to complete offboarding activities.

Offboarding must include, as applicable, revocation of access, return of Company property, confirmation of the return or secure deletion of Company information, resolution of open obligations, transfer of services or data, and retention of required records.

The Company may terminate or suspend a third-party relationship in accordance with the applicable agreement when the third party fails to meet material contractual, security, legal, compliance, or performance obligations.

15. Exceptions

Any exception to this Policy must be requested in writing and approved by _____, with input from _____, _____, _____, or other relevant functions where appropriate.

An exception request must describe the reason for the exception, the risks involved, the duration of the exception, and the compensating controls that will be used to manage the risk. Exceptions are temporary and must be reviewed before expiration.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

16. Training and Awareness

Personnel involved in third-party selection, contracting, management, or oversight must receive training or guidance appropriate to their responsibilities under this Policy.

The Company may provide additional training for personnel responsible for high-risk third-party relationships.

17. Records Retention

The Company will retain third-party records, including risk assessments, due diligence materials, approvals, contracts, monitoring records, remediation plans, and termination records, in accordance with its records retention requirements and applicable legal obligations.

18. Enforcement

Failure to comply with this Policy may result in delayed approval, restricted access, suspension of a third-party relationship, disciplinary action where applicable, or other measures the Company considers appropriate.

19. Policy Administration and Review

_____ is responsible for administering this Policy and may issue procedures, standards, and guidance to support its implementation.

This Policy will be reviewed at least annually and may be amended at any time to reflect changes in business operations, risks, legal requirements, or Company practices. Any amendment must be approved by the designated approval authority.

20. Approval

This Policy is approved and adopted by the undersigned on the Effective Date.

Company

Name _____

Date _____

Signature

_____

Jotform Automatically create polished, fillable and signable documents Clone the document for free!

Jotform

This document is a PDF copy of **Third Party Risk Management Policy** template. You can edit it with **Jotform Sign** and convert to an eSign document with **Jotform Sign**.

Edit PDF

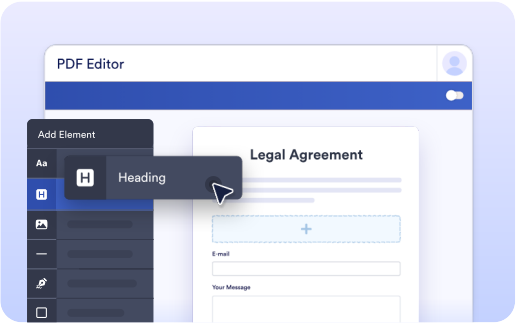
Learn More About Jotform PDF Products

Jotform offers powerful PDF solutions. Check them out below.

Jotform PDF Editor

Turn form submissions into PDFs automatically ready to download or save for your records.

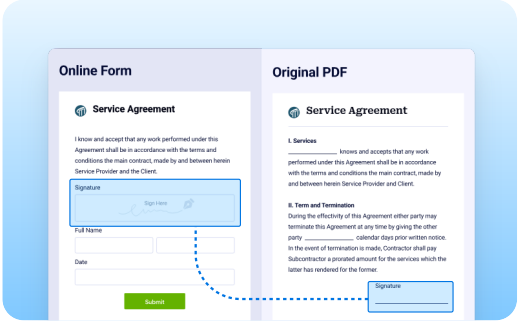
jotform.com/products/pdf-editor/



Smart PDF Forms

Convert your PDF files into online forms that are easy to fill out on any device.

jotform.com/products/smart-pdf-forms/



Jotform Sign

Collect e-signatures with Jotform Sign to automate your signing process.

jotform.com/products/sign/



These templates are suggested forms only. If you're using a form as a contract, or to gather personal (or personal health) info, or for some other purpose with legal implications, we recommend that you do your homework to ensure you are complying with applicable laws and that you consult an attorney before relying on any particular form.