

Vendor Management Policy Template

Replace every [bracketed field] with your own details, delete guidance notes in orange, then have leadership approve and date the final document. This is a template, not legal advice.

Company	[Company name]	Policy owner	[Name, title]
Version	[1.0]	Approved by	[Name, title]
Effective date	[Date]	Next review	[Date, at least annually]

1. Purpose and Scope

This policy defines how [Company] selects, approves, contracts with, onboards, monitors, and exits vendors, so that every vendor has a named owner and every stage leaves auditable evidence.

It applies to all third parties that provide products or services to [Company], including software and cloud providers, contractors, consultants, and agencies. It also applies to free and trial accounts, and to any tool that connects to company systems or handles company or customer data.

Guidance: name free tools, contractors, and open-source services explicitly. Scope gaps are where unmanaged vendors hide.

2. Roles and Responsibilities

Role	Responsibility
Policy Owner ([Security Lead])	Maintains this policy and the Approved Vendor List. Approves vendor requests. Reports on the vendor program to leadership.
Vendor Owner (named person per vendor)	Accountable for the business relationship, annual review, renewal decision, and offboarding of the vendor.
Requesting Employee	Submits a vendor request before purchasing or connecting any third-party product.
Finance / Legal	Confirms budget, reviews contract terms against Section 5, and flags recurring charges not on the Approved Vendor List.
Leadership	Approves this policy and any exception to it.

3. Vendor Request and Approval

- No employee may purchase, subscribe to, or connect a third-party product or service that will access company or customer data without prior approval.
- Requests are submitted to [ticket queue / form link] with the business purpose, data categories involved, and proposed Vendor Owner.
- The Policy Owner assigns a risk tier using [Third-Party Risk Management Policy / tiering method] and records the decision.
- A vendor may only be used once it appears on the Approved Vendor List.

4. Vendor Selection Criteria and the Approved Vendor List

Before approval, the vendor must satisfy the following, proportionate to the data it will access:

- **Business need:** a stated purpose, and confirmation that no existing approved vendor already covers it.
- **Data involved:** data categories shared, matched to the [Data Classification Policy].
- **Security evidence:** a current SOC 2 report, ISO 27001 certificate, or equivalent, dated within [12] months.
- **Continuity and exit:** how company data is exported and deleted if the relationship ends.

The Approved Vendor List is the single source of truth. A vendor not on the list is not approved. Minimum fields:

Vendor	Purpose	Vendor Owner	Data shared	Risk tier	Renewal date	Last review	Report on file
[Name]	[Use]	[Person]	[Categories]	[Tier]	[Date]	[Date]	[Y/N, date]

5. Contract Requirements

Every vendor agreement covering company or customer data must include, at minimum:

- Confidentiality obligations covering company and customer data.
- Security obligations proportionate to the risk of the data involved.
- Notification of a security breach within [72 hours / stated window] of discovery.
- Prior approval for any new subprocessor that will access company data.
- Return and deletion of company data at termination, with written confirmation.
- Delivery of a current compliance report (for example SOC 2) at least [annually].
- Reasonable termination assistance.

A data processing agreement is required where personal data is processed. A business associate agreement is required where the vendor handles protected health information. Deviations follow Section 8.

6. Vendor Onboarding

1. Confirm the approval and signed contract are on file before any account is created or data is shared.
2. Connect through single sign-on where the vendor supports it.
3. Grant least-privilege access scoped to the vendor's purpose.
4. Record the data shared and where it is stored on the Approved Vendor List.
5. Assign a named Vendor Owner.
6. Schedule the first review and record the contract renewal date.

7. Ongoing Review

- The Vendor Owner reviews each vendor with access to customer data at least [annually], and each other vendor at contract renewal.
- A review confirms the vendor is still needed, the compliance report on file is current, access is still appropriate, and the contract terms have not changed.
- An early review is triggered by a security incident at the vendor, a major change in its services or ownership, or the loss of its compliance certification.
- Review outcomes are recorded on the Approved Vendor List.

8. Exceptions

A vendor that cannot meet this policy may be used only under a written exception that states the reason, the compensating controls, an expiry date not longer than [12] months, and approval by [Leadership role]. Exceptions are logged and reviewed at least [quarterly].

9. Offboarding

When a vendor relationship ends, the Vendor Owner must, within [30] days of termination:

1. Revoke all user accounts, API keys, OAuth grants, and integrations, and record the date.
2. Retrieve company data in a usable format before the account closes.
3. Obtain written confirmation that remaining company data has been deleted, on the timeline the contract stated.
4. Update the Approved Vendor List to show the vendor as offboarded, and retain the record for the period defined in the [Data Retention Policy].

10. Policy Review and Enforcement

The Policy Owner reviews this policy at least annually and after any significant change in the vendor landscape or applicable requirements. Violations, including unapproved vendor purchases, are handled under [Company's disciplinary / HR security policy].

Framework Mapping Guide

Framework	Where it applies	What it expects	Sections above
SOC 2	Common Criteria CC9.2	The entity assesses and manages risks associated with vendors and business partners.	3, 4, 6, 7
ISO 27001:2022	Annex A 5.19 to 5.23	Supplier relationships, supplier agreements, ICT supply chain, monitoring and change management of supplier services, cloud services.	3 to 9
HIPAA	45 CFR 164.308(b), 164.314(a)	Written contract with each business associate covering Security Rule compliance, subcontractors, and incident reporting.	5, 9
GDPR	Article 28	Binding contract with each processor; documented instructions; approval for sub-processors.	5, 6
PCI DSS 4.0	Requirement 12.8	List of third-party service providers, written agreements, due diligence before engagement, annual compliance monitoring.	4, 5, 7

Verify clause references against the current published text of each framework before relying on this table in an audit. Need a hand turning this policy into enforced, evidence-backed controls? [Book a free demo at calendly.com/complyjet/demo](https://calendly.com/complyjet/demo).