

Vendor Management Policy

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	[Version]

1. Purpose and scope

This policy supports the SOC 2 common criteria CC9.2 by establishing vendor risk management requirements.

This policy applies to all third-party vendors and subservice organizations.

2. Vendor tiers

Vendors are tiered by what they can reach, not by what they cost. The tier sets how much assurance is collected and how often the vendor is reviewed.

Tier	What the vendor can reach	Assurance collected	Review
1, critical	Customer data, production systems, the identity provider or source code	A current SOC 2 report or equivalent, plus the security questionnaire where the report leaves gaps	Every 12 months
2, limited	Internal company data only, with no production access	The shorter security questionnaire	Every 24 months
3, peripheral	No company data and no access to Company systems	A register entry only	When its reach changes

3. Vendor risk assessment

- Vendors are assessed for risk before onboarding and again on the review schedule for their tier.
- Critical vendors provide a current SOC 2 report or equivalent assurance, reviewed every 12 months.

- Where a critical vendor has no SOC 2 report or equivalent, it completes the security questionnaire in writing, and the decision to proceed is recorded as a policy exception with its reason, its approver and a date to look again.

4. Contracts

Contracts with Tier 1 vendors include:

- A security incident notice period, stated in hours.
- Confidentiality of Company and customer data.
- Deletion or return of data when the contract ends.
- Notice before a new subprocessor handles Company data.
- The right to ask for updated assurance each year.

5. Vendor register

Every vendor is recorded in [Vendor register location] before it is used. Each entry names the service, the data it can reach, its tier, an internal owner, the assurance collected and the date of the last review.

6. Reviewing a vendor report

1. Confirm the report is current, covers the service you use and was issued by a licensed CPA firm.
2. Read the opinion and any exceptions, and decide whether they affect you.
3. Read the complementary user entity controls and assign each one to an owner at the Company.
4. Record the review with the reviewer, the date and the conclusion.

7. Ending a vendor relationship

When a vendor is retired, its access is removed, the return or deletion of Company data is confirmed in writing, and the register entry is closed with the date.

8. Roles and responsibilities

Role	Held by	Responsibility
Policy approver	[Policy approver role]	Approves this policy, each new version, and any risk the Company accepts instead of meeting it.
Policy owner	[Security owner role]	Maintains this policy, makes sure the controls in it operate, keeps the evidence, and reviews it at least once a year.

Role	Held by	Responsibility
Vendor owner	The employee who requests the vendor	Supplies the information for the assessment and the register, and tells the policy owner when the vendor reach changes.
All personnel	Everyone in scope	Follow this policy and report a suspected breach of it to the [Security owner role].

9. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

Record	What it shows	Where it is kept
Approved policy	This document, signed by the approver, with its version history.	[Documentation system]
Vendor register	List of vendors and their risk ratings.	[Documentation system]
Vendor SOC 2 reports	Audit reports for critical vendors.	[Evidence storage location]
Vendor review notes	Who reviewed each report or questionnaire, when, and what they concluded.	[Evidence storage location]

10. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

11. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

Version	Date	Summary of change	Approved by
[Version]	[Effective date]	First version.	[Policy approver role]

Policy approver

Name:

Signature:

Date:

12. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Effective date]	The date the approver signs this version.
[Version]	Start at 1.0 and increase it each time the document changes.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Policy approver role]	The officer who approves policies and accepted risks, for example Chief Executive Officer.
[Evidence storage location]	The shared folder or system where evidence is kept.
[Documentation system]	Where policies and procedures are published, for example the company wiki.
[Vendor register location]	Where the vendor register is kept.
[Evidence retention period]	How long audit evidence is kept, for example three years.

Field	What to enter
[Next review date]	The date this version must be reviewed by, at most 12 months after the effective date.

Source

Source: free template from www.polaralabs.com/templates/vendor-management-policy (CC BY 4.0).