

Vendor Risk Management Policy

Purpose

Your Organization relies on third-party vendors — SaaS platforms, cloud providers, processors, professional services firms, and software suppliers — to deliver its products and operate its business. Every vendor relationship that touches Your Organization data or systems extends the Your Organization attack surface. This policy establishes a consistent approach to identifying, assessing, and continuously monitoring that risk before and throughout a vendor relationship.

Scope

This policy applies to every third party that stores, processes, transmits, or accesses Your Organization information; every third party that integrates with Your Organization production systems; and every third party whose failure would materially disrupt Your Organization's ability to operate. It applies across the full vendor lifecycle: due diligence, contracting, onboarding, ongoing monitoring, and offboarding.

Vendor tiering

Vendors are tiered based on the sensitivity of data they handle, the privilege of access granted, and business criticality.

Tier	Description	Examples
Tier 1 — Critical	Handles Restricted data, has privileged production access, or is mission critical	Cloud provider, payments processor, identity provider, core database managed service
Tier 2 — Important	Handles Confidential data or supports important business functions	Email and productivity suite, customer support platform, analytics
Tier 3 — Standard	Handles Internal data or poses limited risk	Marketing automation, non-sensitive SaaS
Tier 4 — Minimal	No access to Your Organization data; low business impact	Office supply and facilities vendors

Pre-engagement due diligence

Before contracting with a Tier 1 or Tier 2 vendor, the requester must submit a vendor assessment to the security team. The assessment reviews:

- **Security attestations.** SOC 2 Type II, ISO 27001, PCI DSS, or HITRUST reports as applicable to the service provided and data handled. Reports must be current (issued within the last 12 months).

- **Gap review.** Security reviews the attestation(s), notes carve-outs and qualifications, and records compensating controls for any material gaps.
- **Privacy and data protection.** Where the vendor will process personal data, Legal confirms the appropriate DPA, sub-processor commitments, and cross-border transfer mechanisms are in place.
- **Questionnaire.** Where a recognized attestation is not available, the vendor completes a security questionnaire (SIG-Lite, CAIQ, or Your Organization's standard) and evidence is reviewed.
- **Architecture review.** For Tier 1 vendors handling Restricted data or taking privileged production access, a security architecture review is conducted.

Vendor engagement may not proceed until the assessment is approved by the security team and, for Tier 1 vendors, signed off by the CISO or designee.

Contractual requirements

Contracts with Tier 1 and Tier 2 vendors must include: confidentiality obligations; security standards the vendor will maintain; incident notification timing (no later than 72 hours absent contractual urgency); audit or evidence rights; sub-processor flow-down; data protection addenda where applicable; and termination-assistance and data-return obligations.

Ongoing monitoring

- **Tier 1 vendors.** Annual re-review of current SOC 2 / ISO / PCI attestations. Security checks for known breaches, changes in sub-processors, and material service changes at least quarterly.
- **Tier 2 vendors.** Annual re-review of attestations. Ad-hoc monitoring for news of vendor security incidents.
- **Tier 3 vendors.** Biennial re-review.
- **All tiers.** A vendor breach notification from the vendor opens an incident in Your Organization's incident process; the vendor owner participates in the response.

Inventory

Security maintains an authoritative vendor inventory capturing: legal name, service description, tier, data classifications handled, primary owner at Your Organization, contract term, last review date, and links to the current attestation. The inventory is updated at onboarding, tier change, material service change, and offboarding.

Offboarding

When a vendor relationship ends, the vendor owner coordinates with security and IT to: revoke all access, recover or destroy data per contract (with evidence), terminate integrations and API keys, and close the inventory record with a terminal note.

Scope exceptions

Business-driven urgency is not a substitute for diligence. Exceptions — for example, engaging a vendor under an attestation carve-out or with an expired report — must be approved by the CISO or designee, documented, and time-bound.

Review cadence

This policy is reviewed annually by the security team and the vendor management function, or sooner if Your Organization's regulatory obligations or the vendor landscape materially change.

Effective date: [the date this policy takes effect]