Capital Investment Club

Third Party Risk Management Policy

Third-party classification, onboarding diligence, monitoring, evidence, exceptions, and offboarding.

Owner: Security and Operations Status: Published Last updated: June 8, 2026 Review cadence: Annual or after material vendor, product, regulatory, or security changes

Purpose

This policy defines how Capital Investment Club evaluates, approves, monitors, and offboards third parties that may support CIC operations, process CIC data, access CIC systems, or materially affect customer, financial, security, privacy, or operational risk.

Scope

This policy applies to vendors, contractors, service providers, cloud providers, payment providers, identity providers, banking and financial data providers, analytics tools, support tools, and any other third party that CIC uses to operate the platform.

Risk Tiers

Third parties must be classified before onboarding:

Tier	Description	Examples
Critical	Provider supports production financial, identity, wallet, payment, banking, KYC/KYB, or security operations.	Payment processors, banking data providers, cloud hosting, identity verification.
High	Provider stores or processes sensitive CIC, customer, employee, or platform data.	Support tooling, email/SMS providers, analytics with user identifiers.
Moderate	Provider supports business operations with limited sensitive data exposure.	Project management, collaboration, operational SaaS.
Low	Provider has minimal data access and no production or sensitive workflow dependency.	Public reference tools or non-sensitive utilities.

Onboarding Controls

Before a third party is approved, CIC should document:

- Business owner and technical owner.
- Intended use, systems impacted, and data categories processed.
- Risk tier and rationale.

- Security and privacy review evidence appropriate to the risk tier.
- Contract, data processing, confidentiality, incident notification, and termination expectations.
- Access method, least-privilege configuration, and authentication requirements.
- Monitoring, renewal, and reassessment cadence.

Required Evidence

Evidence may include security questionnaires, SOC 2 or equivalent reports, privacy policies, data processing terms, penetration test summaries, cloud/security architecture notes, incident history, compliance attestations, configuration screenshots, access-control evidence, and approval records.

Ongoing Monitoring

Critical and high-risk third parties should be reviewed at least annually. Reviews should confirm:

- Continued business need.
- Current access level and owners.
- Contract and data processing status.
- Security posture or available assurance evidence.
- Open incidents, findings, exceptions, or remediation items.
- Vendor status, product changes, and material risk changes.

Offboarding

When a third party is no longer required, CIC should:

- Disable accounts, tokens, API keys, webhooks, and integrations.
- Revoke data access and production access.
- Export or preserve required evidence and records.
- Confirm deletion or return of CIC data where contractually required.
- Update the vendor inventory, risk register, and evidence calendar.

Exceptions

Exceptions must identify the business need, risk owner, compensating controls, expiration date, and approval. Critical or high-risk exceptions should be reviewed by security and leadership before acceptance.

Relationship To Vendor Risk

This document is the canonical third-party risk policy. The Vendor Risk Management Policy remains a supporting operating reference for vendor-specific diligence and lifecycle details.