Vendor Risk Management Policy

Third-Party and Fourth-Party Risk Management

Version: 1.1 **Date:** August 2026 **Classification:** Public

Executive Summary

ScamZero maintains a limited vendor footprint by design. This document outlines how we evaluate, monitor, and manage third-party vendors to address "fourth-party risk" concerns.

- Every third party that receives any data is named in the ScamZero Subprocessor List, which is the single source of truth for this question
- All critical vendors maintain SOC 2 Type II certification
- No customer data shared with vendors except for core service delivery
- Annual vendor reviews and continuous monitoring

Policy Purpose & Scope

Purpose

This policy establishes ScamZero's approach to identifying, assessing, and managing risks associated with third-party vendors. It ensures that vendors who may access, process, or store data on our behalf maintain appropriate security controls.

Scope

This policy applies to:

- Infrastructure and platform providers
- AI/ML service providers
- Payment processors
- Any vendor that processes, stores, or transmits data on ScamZero's behalf

Vendor Classification

Risk-Based Classification

Category	Definition	Due Diligence	Review Frequency
CRITICAL	Vendors essential to service delivery or handling sensitive data	SOC 2 Type II required, security questionnaire, contract review	Annual
HIGH	Vendors with access to non-sensitive operational data	SOC 2 or equivalent required, contract review	Annual
STANDARD	Vendors providing non-critical services with no data access	Basic due diligence	As needed

Current Critical Vendors

Vendor	Service	Data Processed	Certifications
Cloudflare, Inc.	Infrastructure (Workers, D1, R2, Pages, DNS, Turnstile)	All application data, encrypted at rest and in transit	SOC 2 Type II, ISO 27001, PCI DSS
Cloudflare, Inc.	Workers AI — scam analysis	Submitted text and screenshots, processed in memory and never written to storage	SOC 2 Type II, ISO 27001
Google LLC	Web Risk API — URL threat detection	The complete submitted URL, sent in full rather than hashed	SOC 2 Type II, ISO 27001, FedRAMP
Twilio SendGrid	Email delivery (admin notifications, invitations)	Email addresses and message content for delivery only	SOC 2 Type II, ISO 27001
Stripe, Inc.	Payment processing (ScamZero billing only)	ScamZero customer payment info (not end-user data)	SOC 2 Type II, PCI DSS Level 1

Minimal Data Sharing

Account numbers, government-issued identifiers, and student education records is **never shared with vendors**. Content submitted for scam analysis is processed by Cloudflare Workers AI. Cloudflare does not retain inputs and does not use them to train models. SendGrid receives only email addresses for delivery purposes. URLs submitted for analysis are checked via Google Web Risk API.

Vendor Due Diligence Process

Pre-Engagement Assessment

Before engaging a new critical or high-risk vendor, ScamZero requires:

- ✓ **Security Certification Review:** SOC 2 Type II or equivalent
- ✓ **Privacy Policy Review:** Data handling and retention practices
- ✓ **Contract Review:** Security obligations, breach notification, data handling
- ✓ **Insurance Verification:** Adequate cyber liability coverage
- ✓ **Subprocessor Review:** Understanding of vendor's own third parties

Required Contract Provisions

All critical vendor contracts must include:

- Data protection and confidentiality obligations
- 72-hour breach notification requirement
- Right to audit or receive audit reports
- Data return/deletion upon termination
- Compliance with applicable regulations

Ongoing Monitoring

Continuous Monitoring Activities

Activity	Frequency	Responsibility
SOC 2 report review	Annual	Security Lead
Vendor status page monitoring	Continuous	Engineering
Security incident notification review	As received	Security Lead
Contract renewal review	At renewal	CEO
Subprocessor list changes	As notified	Security Lead

Vendor Performance Metrics

- Uptime and availability (per SLA)
- Security incident history
- Response time for security inquiries
- Certification currency

Vendor Termination & Exit

Exit Planning

For critical vendors, ScamZero maintains:

- Data export capabilities and procedures
- Alternative vendor assessment (where feasible)
- Transition timeline requirements

Data Handling at Termination

- Confirmation of data deletion from vendor systems
- Return of any data in usable format
- Certificate of destruction for sensitive data

Policy Governance

Role	Responsibility
CEO	Policy approval, critical vendor relationship ownership
Security Lead	Due diligence execution, ongoing monitoring, policy maintenance
Engineering Lead	Technical assessment, integration security review

Policy Review

This policy is reviewed annually or when significant changes occur to vendor relationships or regulatory requirements.

Questions?

For vendor risk inquiries, contact security@scamzero.com

ScamZero

Vendor Risk Management Policy

Version 1.1 | August 2026