HECVAT Lite Assessment

Higher Education Community Vendor Assessment Toolkit

Vendor: ScamZero   **Version:** 1.0   **Date:** February 2026

Vendor Information

Company Name	ScamZero
Product/Service Name	ScamZero Scam Safety Platform
Website	https://scamzero.com
Primary Contact	support@scamzero.com
Service Description	A white-labeled scam safety platform that helps community members check messages for scams (emails, texts, screenshots), access educational content about current threats, and get guidance if they've fallen victim.

COMP – Company Information

COMP-01

Does your organization have a dedicated information security team or officer?

> **Yes.** ScamZero maintains dedicated security oversight with regular security reviews and monitoring.

COMP-02

Does your organization carry cyber liability insurance?

> **Yes.** ScamZero maintains cyber liability insurance coverage.

COMP-03

Does your organization have a written information security policy?

> **Yes.** See attached Information Security Policy document.

DCTR – Documentation

DCTR-01

Can you provide documentation of your security practices upon request?

> **Yes.** Security documentation is available upon request under NDA.

DCTR-02

Do you have a privacy policy publicly available?

> **Yes.** Available at scamzero.com/privacy

DATA – Data Handling

DATA-01

What types of data does your application/service collect or process?

> ScamZero processes:
>
> - Email content forwarded by users for analysis
> - Uploaded screenshot images (of texts, DMs, or suspicious messages)
> - AI chat conversations (for scam-related questions)
> - Admin email addresses for organization account management
>
> **Note:** Portal end-users are anonymous - no member accounts required. No student records, grades, or FERPA-protected educational data is collected.

DATA-02

How long is data retained?

> **12 hours for confirmed submissions.** Confirmed email content, screenshots, and assessments are automatically deleted within 12 hours. Pending (unconfirmed) email submissions are deleted within 7 days. AI chat conversations are retained by Zapier for 30 days. Admin accounts remain until deletion is requested.

DATA-03

Is data encrypted at rest?

> **Yes.** All data is encrypted at rest using AES-256 encryption via Cloudflare's infrastructure.

DATA-04

Is data encrypted in transit?

Yes. All data is transmitted over TLS 1.3.

DATA-05

Can users request deletion of their data?

Yes. Users can request complete data deletion through the portal or by contacting support. Deletion is processed within 48 hours.

DATA-06

Where is data stored geographically?

Data is stored in Cloudflare's global network with primary processing in the United States. Data does not leave U.S. jurisdiction.

ACCS – Access Control

ACCS-01

Does the application support role-based access control?

> **Yes.** Organization portals support multiple permission levels: owner, admin, and member roles with granular permissions.

ACCS-02

Does the application support Single Sign-On (SSO)?

> **Not applicable.** ScamZero's portal end-users are anonymous (no accounts required). Admin accounts are limited to a small number of organizational administrators where SSO integration provides minimal benefit.

ACCS-03

Does the application support Multi-Factor Authentication (MFA)?

> **Not applicable.** End-users access ScamZero anonymously without accounts. Admin authentication uses passwordless magic links, which provide similar security to MFA.

ACCS-04

Are passwords stored securely?

> **Yes.** ScamZero uses passwordless authentication (magic links). No passwords are stored.

THRD – Third Parties

THRD-01

What third-party services does your application use?

- **Cloudflare:** Hosting, database, CDN, and security (SOC 2 Type II certified)
- **Google Gemini AI:** AI analysis for scam detection (ISO 27001 certified)
- **SendGrid:** Transactional email delivery (SOC 2 Type II certified)
- **Google Safe Browsing:** URL threat intelligence
- **Zapier:** AI chatbot service (30-day data retention)

THRD-02

Do subprocessors have access to customer data?

Yes, limited. Google Gemini AI processes email content for analysis only. Data is not retained by Google beyond the API call. Zapier processes AI chat conversations with 30-day retention. See vendor data processing terms.

INCR – Incident Response

INCR-01

Do you have an incident response plan?

> **Yes.** ScamZero maintains a documented incident response plan with defined roles and escalation procedures.

INCR-02

Will you notify customers of security breaches affecting their data?

> **Yes.** Affected customers will be notified within 72 hours of confirmed breach discovery, as required by applicable regulations.

VULN – Vulnerability Management

VULN-01

Do you perform regular security testing?

> **Yes.** Regular security reviews and dependency scanning are performed. Cloudflare provides additional DDoS protection and WAF capabilities.

VULN-02

Do you have a vulnerability disclosure program?

> **Yes.** Security researchers can report vulnerabilities to support@scamzero.com.

AVLB – Availability

AVLB-01
What is your target uptime/availability?

99.9% uptime target. Service runs on Cloudflare's globally distributed infrastructure.

AVLB-02
Do you have a disaster recovery plan?

Yes. Data is replicated across Cloudflare's global network. Database backups are maintained with point-in-time recovery capability.

FERPA Applicability

FERPA-01

Does this service process student education records?

> **No.** ScamZero does not collect, store, or process student education records, grades, transcripts, or any FERPA-protected information. The service analyzes email content solely for scam detection purposes.

FERPA-02

Can the service be configured to exclude student data?

> **N/A.** No student education records are processed. Users choose what emails to submit for analysis.