Information Security Policy

Data Protection, Access Control, and Incident Response

Version: 1.0 **Date:** February 2026

Table of Contents

1. Purpose and Scope

1.1 Purpose

This Information Security Policy establishes the security requirements and practices for the ScamZero Scam Safety Platform. It ensures the confidentiality, integrity, and availability of customer data and service operations.

1.2 Scope

This policy applies to:

- All ScamZero systems, applications, and infrastructure
- All employees, contractors, and third-party service providers
- All customer data processed by ScamZero services

1.3 Policy Statement

> ScamZero is committed to protecting customer data through appropriate technical and organizational security measures. We process data only as necessary to provide our scam detection service and delete it promptly after analysis.

2. Security Governance

2.1 Security Oversight

ScamZero maintains dedicated security oversight with responsibility for:

- Implementing and maintaining security controls
- Conducting security reviews and assessments
- Managing security incidents
- Ensuring regulatory compliance

2.2 Policy Review

This policy is reviewed annually or when significant changes occur to the service, threat landscape, or regulatory requirements.

2.3 Compliance

ScamZero's security program is designed to support compliance with:

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- Higher education security requirements (HECVAT)
- Financial services requirements (GLBA, NCUA)
- Industry best practices (OWASP, CIS)

3. Data Classification

3.1 Classification Levels

Level	Description	Examples	Handling
Confidential	Customer data requiring highest protection	Email content, attachments, credentials	Encrypted, 12-hour deletion, access logged
Internal	Business data not for public disclosure	API keys, system configurations, analytics	Encrypted, access restricted
Public	Information intended for public access	Website content, public documentation	No special handling required

3.2 Data Retention

Data Type	Retention Period
Email content and assessments	12 HOURS (AUTO-DELETED)
Screenshot images	12 HOURS (AUTO-DELETED)
Pending email submissions	7 DAYS (AUTO-DELETED)
AI chat conversations	30 DAYS (ZAPIER)
User account data	UNTIL DELETION REQUESTED
System logs	30 DAYS

4. Access Control

4.1 Principles

- ✓ **Least Privilege:** Users receive minimum access necessary for their role
- ✓ **Need-to-Know:** Access to confidential data is restricted to those who require it
- ✓ **Separation of Duties:** Critical functions require multiple approvals

4.2 Authentication

- Passwordless authentication via magic links (no passwords to compromise)
- JWT tokens for session management with appropriate expiration
- Email verification required for account activation
- Administrative access requires additional authentication

4.3 Authorization

- Role-based access control (RBAC) for organization portals
- Granular permissions (scam alerts, settings, billing, user management)
- API endpoints protected with authentication and rate limiting

4.4 Access Review

Access rights are reviewed quarterly and upon role changes or termination.

5. Encryption

5.1 Data in Transit

- ✓ All connections use TLS 1.3
- ✓ HTTPS enforced for all web traffic
- ✓ API communications encrypted end-to-end
- ✓ Email submissions processed over secure channels

5.2 Data at Rest

- ✓ Database encryption using AES-256 (Cloudflare D1)
- ✓ Object storage encryption (Cloudflare R2)
- ✓ Encryption keys managed by cloud provider with appropriate controls

5.3 Key Management

- API keys and secrets stored in environment variables
- Secrets never committed to source control
- Regular rotation of sensitive credentials

6. Infrastructure Security

6.1 Cloud Infrastructure

ScamZero runs on Cloudflare's infrastructure, which provides:

- ✓ SOC 2 Type II certification
- ✓ ISO 27001 certification
- ✓ Global DDoS protection
- ✓ Web Application Firewall (WAF)
- ✓ Geographic distribution for availability

6.2 Network Security

- All services behind Cloudflare's security layer
- Rate limiting on all API endpoints (30 requests/minute)
- Bot protection and challenge mechanisms
- Service-to-service authentication for internal communications

6.3 Monitoring

- Real-time logging of all API requests
- Error tracking and alerting
- Performance monitoring
- Security event logging

7. Secure Development

7.1 Development Practices

- ✓ Security considered in design phase
- ✓ Input validation on all user inputs
- ✓ Output encoding to prevent XSS
- ✓ Parameterized queries to prevent SQL injection
- ✓ CORS policies restricting cross-origin access

7.2 Code Review

- All code changes reviewed before deployment
- Security-focused review for sensitive functions
- Automated security scanning in CI/CD pipeline

7.3 Dependency Management

- Regular updates of third-party dependencies
- Vulnerability scanning of dependencies
- Minimal use of external packages

8. Incident Response

8.1 Incident Classification

Severity	Description	Response Time
Critical	Active breach, data exposure, service down	Immediate
High	Potential breach, significant vulnerability	4 hours
Medium	Minor vulnerability, isolated issue	24 hours
Low	Informational, no immediate risk	5 business days

8.2 Response Procedures

1. **Detection:** Identify and verify the incident
2. **Containment:** Isolate affected systems
3. **Eradication:** Remove the threat
4. **Recovery:** Restore normal operations
5. **Post-Incident:** Document lessons learned

8.3 Breach Notification

⚠️ Notification Commitment

In the event of a confirmed data breach affecting customer data:

- Affected customers notified within 72 hours
- Relevant regulatory authorities notified as required
- Documentation of incident and response maintained

8.4 Security Contact

Report security vulnerabilities to: **support@scamzero.com**

9. Vendor Management

9.1 Third-Party Services

Vendor	Purpose	Certifications
Cloudflare	Infrastructure, CDN, security	SOC 2 ISO 27001
Google Gemini AI	AI analysis	SOC 2 ISO 27001
Google Safe Browsing	URL threat intelligence	PUBLIC API
SendGrid	Transactional email	SOC 2
Zapier	AI chatbot service	SOC 2

9.2 Vendor Requirements

- ✓ Security certifications required for data processors
- ✓ Data processing agreements in place
- ✓ Regular review of vendor security posture

10. Business Continuity

10.1 Availability

- ✓ Target uptime: 99.9%
- ✓ Globally distributed infrastructure
- ✓ Automatic failover capabilities

10.2 Backup and Recovery

- Database backups with point-in-time recovery
- Configuration stored in version control
- Recovery procedures documented and tested

10.3 Data Portability

Users can export their account data upon request. Note that email content is deleted within 12 hours and cannot be recovered after deletion.

Document Control

Version	Date	Changes
1.0	February 2026	Initial release

For questions, contact: support@scamzero.com

Document Version 1.0 | February 2026