Incident Response Plan

Security Incident Detection, Response & Recovery Procedures

Version: 1.0 **Date:** April 2026 **Classification:** Confidential

Purpose & Scope

This Incident Response Plan (IRP) establishes procedures for detecting, responding to, and recovering from security incidents affecting ScamZero systems or customer data.

Scope: All ScamZero systems, data, and personnel.

Incident Classification

Severity Levels

Severity	Definition	Examples	Response Time
CRITICAL	Active breach, data exfiltration, or complete service outage	Unauthorized data access, ransomware, DDoS	< 15 minutes
HIGH	Potential breach, significant vulnerability, or partial outage	Suspicious access patterns, critical CVE	< 1 hour
MEDIUM	Security anomaly, minor vulnerability, or degraded service	Failed login attempts, minor bug	< 4 hours
LOW	Informational, no immediate risk	Security scan, phishing attempt blocked	< 24 hours

NCUA Reporting Requirements

Per NCUA cyber incident reporting requirements, the following must be reported to affected credit union customers within **72 hours**:

- Unauthorized access to member data
- Ransomware or malware infection
- Disruption caused by third-party compromise
- Any incident materially impacting operations

Incident Response Team

Core Team

Role	Responsibility
Incident Commander	Overall coordination, decision authority (CEO)
Technical Lead	Investigation, containment, recovery (Engineering Lead)
Communications Lead	Customer & stakeholder communication (CEO)

External Resources

Resource	Purpose
Cloudflare Support	Infrastructure incidents (Enterprise support portal)
Legal Counsel	Regulatory compliance, breach notification
Cyber Insurance	Claims, forensics resources

Phase 1: Detection & Identification

Objective: Identify and confirm the incident.

Detection Sources

- Cloudflare security alerts
- Application error monitoring
- Customer reports
- Automated anomaly detection
- Third-party notifications

Actions

1. Acknowledge alert within response time SLA
2. Gather initial information (what, when, scope)
3. Classify severity level
4. Activate Incident Response Team if severity ≥ High

Phase 2: Containment

Objective: Limit the impact and prevent further damage.

Immediate Actions

- Isolate affected systems (if applicable)
- Revoke compromised credentials
- Block malicious IPs/actors
- Preserve evidence (logs, snapshots)

Short-Term Containment

- Deploy temporary fixes
- Enable additional monitoring
- Notify Cloudflare if infrastructure-level issue

Phase 3: Eradication

Objective: Remove the threat and close vulnerabilities.

Actions

1. Identify root cause
2. Remove malicious code/access
3. Patch vulnerabilities
4. Verify no persistence mechanisms remain
5. Update security controls

Phase 4: Recovery

Objective: Restore normal operations safely.

Actions

1. Restore from clean backups if needed
2. Verify system integrity
3. Monitor for recurrence
4. Gradually restore full service
5. Confirm with Incident Commander before declaring resolved

Phase 5: Post-Incident Review

Objective: Learn and improve.

Timeline: Complete within 5 business days of resolution.

Deliverables

- ✓ Incident timeline
- ✓ Root cause analysis
- ✓ Impact assessment
- ✓ Lessons learned
- ✓ Remediation actions
- ✓ Process improvements

Customer Notification Procedures

Notification Timeline

Incident Type	Notification Deadline	Method
Data breach affecting customer data	**72 hours**	Email + phone call
Service disruption > 4 hours	4 hours	Email
Security vulnerability (no breach)	5 business days	Email

Notification Content

All breach notifications will include:

- Description of the incident
- Date/time of discovery
- Types of data potentially affected
- Steps taken to address the incident
- Recommended actions for the customer
- ScamZero contact for questions

Regulatory Notifications

For credit union customers, ScamZero will:

- Provide information needed for NCUA reporting
- Cooperate with customer's regulatory obligations
- Support customer's member notification if required

Evidence Preservation

Evidence to Preserve

- System logs (Cloudflare, application)
- Access logs and authentication records
- Network traffic data
- Database query logs
- Screenshots and documentation
- Communication records

Chain of Custody

- All evidence timestamped and hashed
- Access limited to Incident Response Team
- Transfer documented if shared with third parties
- Retained for minimum 1 year post-incident

Training & Testing

Training

- All personnel: Annual security awareness training
- Incident Response Team: Quarterly IRP review
- New hires: IRP orientation within 30 days

Testing

- **Tabletop Exercise:** Annual simulation of incident scenario
- **Plan Review:** Annual review and update of this document
- **Post-Incident:** Update IRP based on lessons learned

Emergency Contact

Email: security@scamzero.com