Incident Response Plan

RichesReach Security Operations

Version: 1.0
Last Updated: 2026
Owner: Security Team
Review Frequency: Quarterly

Overview

This plan outlines the procedures for detecting, responding to, and recovering from security incidents affecting RichesReach systems, data, or users.

Incident Classification

Severity Levels

Level	Description	Response Time	Escalation
Critical	Active breach, data exfiltration, service disruption	Immediate	CTO + Legal + PR
High	Potential breach, suspicious activity, vulnerability exploitation	1 hour	Security Lead + Engineering
Medium	Security event, policy violation, suspicious login	4 hours	Security Team

Level	Description	Response Time	Escalation
Low	Security alert, failed authentication, minor policy violation	24 hours	Security Team

---

Roles & Responsibilities

Incident Commander

- **Role:** Overall incident coordination
- **Who:** Security Lead or CTO
- **Responsibilities:**
- Coordinate response activities
- Make critical decisions
- Communicate with stakeholders

Security Team

- **Role:** Technical investigation and remediation
- **Who:** Security engineers
- **Responsibilities:**
- Investigate security events
- Contain threats
- Remediate vulnerabilities
- Document findings

Engineering Team

- **Role:** Technical support and fixes
- **Who:** Backend/frontend engineers
- **Responsibilities:**

- Implement fixes
- Deploy patches
- Restore services

Legal/Compliance

- **Role:** Regulatory and legal guidance
- **Who:** Legal counsel
- **Responsibilities:**
- Regulatory notification requirements
- Data breach notification (if applicable)
- Contractual obligations

Communications

- **Role:** External and internal communications
- **Who:** PR/Marketing lead
- **Responsibilities:**
- Customer notifications
- Public statements
- Internal communications

Incident Response Phases

Phase 1: Detection

Sources: - Security event logs (SecurityEvent model) - Sentry error tracking - AWS CloudWatch alarms - User reports - External threat intelligence

Detection Triggers: - Unusual login patterns - Failed authentication spikes - Unauthorized access attempts - Data exfiltration indicators - Service anomalies

Actions: 1. Log incident in security tracking system 2. Assign severity level 3. Notify Incident Commander 4. Begin initial investigation

---

Phase 2: Containment

Immediate Containment (Critical/High): - Isolate affected systems - Revoke compromised credentials - Block malicious IPs - Disable affected user accounts - Enable additional monitoring

Long-term Containment: - Patch vulnerabilities - Update security controls - Enhance monitoring - Implement compensating controls

---

Phase 3: Eradication

Actions: - Remove threat from environment - Patch all vulnerabilities - Update security configurations - Remove backdoors/malware - Verify clean state

---

Phase 4: Recovery

Actions: - Restore services from clean backups - Verify system integrity - Re-enable services gradually - Monitor for recurrence

---

Phase 5: Post-Incident

Actions: - Document incident timeline - Conduct post-mortem - Identify root causes - Update security controls - Update this plan - Share lessons learned

---

Communication Templates

Internal Notification (Critical)

```
Subject: [CRITICAL] Security Incident - [Brief Description]

Incident ID: INC-2026-XXX
```

```
Severity: Critical
Status: Under Investigation

Summary:
[Brief description of incident]

Actions Taken:
- [Containment actions]
- [Investigation steps]

Next Steps:
- [Remediation plan]
- [Timeline]

Contact: [Incident Commander]
```

Customer Notification (Data Breach)

```
 Subject: Important Security Update

Dear [Customer],

We are writing to inform you of a security incident that may have affected your acco

What Happened:
[Clear, non-technical description]

What We're Doing:
- [Remediation steps]
- [Preventive measures]

What You Should Do:
- [User actions: change password, enable 2FA, etc.]

For Questions:
[Support contact]
```

```
We take security seriously and apologize for any concern this may cause.

RichesReach Security Team
```

Runbook Checklists

Checklist: Unauthorized Access

- [ ] Confirm incident and assign severity
- [ ] Revoke compromised credentials
- [ ] Review access logs for affected account
- [ ] Identify data accessed
- [ ] Contain threat (block IPs, disable account)
- [ ] Notify affected users (if data accessed)
- [ ] Document incident
- [ ] Update security controls

Checklist: Data Breach

- [ ] Confirm breach and scope
- [ ] Contain breach (isolate systems)
- [ ] Assess data accessed
- [ ] Notify legal/compliance
- [ ] Determine regulatory notification requirements
- [ ] Prepare customer notification
- [ ] Notify law enforcement (if required)
- [ ] Document incident
- [ ] Conduct post-mortem

Checklist: DDoS Attack

- [ ] Confirm attack (not legitimate traffic)
- [ ] Enable DDoS protection (AWS Shield)

- [ ] Block malicious IPs
- [ ] Scale infrastructure if needed
- [ ] Monitor traffic patterns
- [ ] Document attack characteristics
- [ ] Update WAF rules
- [ ] Post-incident review

Tools & Resources

Incident Tracking

- **Tool:** GitHub Issues (security label) or Jira
- **Template:** See incident template below

Communication

- **Slack:** #security-incidents channel
- **Email:** security-incident@richesreach.com
- **PagerDuty:** On-call rotation

Investigation Tools

- AWS CloudWatch Logs
- Django SecurityEvent logs
- Sentry error tracking
- Database query logs
- Network traffic logs

Tabletop Exercise

Frequency: Quarterly
Duration: 2 hours
Participants: Security Team, Engineering Lead, CTO

Scenario: Unauthorized access to user account with financial data

Exercise Steps: 1. Detection: Review security event logs 2. Containment: Revoke credentials, block IP 3. Investigation: Trace access, identify data accessed 4. Notification: Draft customer communication 5. Remediation: Patch vulnerability, update controls 6. Post-mortem: Document lessons learned

Last Exercise: [Date]
Next Exercise: [Date + 3 months]

Regulatory Requirements

GDPR (EU Users)

- **Notification:** Within 72 hours to supervisory authority
- **User Notification:** Without undue delay if high risk
- **Documentation:** Maintain incident log

CCPA (California Users)

- **Notification:** Within reasonable time
- **Content:** Description, date range, data types
- **Remediation:** Offer identity theft protection if applicable

FINRA (If Applicable)

- **Notification:** Within 30 days
- **Content:** Incident details, remediation steps
- **Documentation:** Maintain records for 6 years

Continuous Improvement

Quarterly Review: - Review all incidents from quarter - Identify patterns - Update response procedures - Update this plan - Schedule next tabletop exercise

Metrics: - Mean time to detection (MTTD) - Mean time to containment (MTTC) - Mean time to resolution (MTTR) - Incident count by severity - False positive rate

---

Contact Information

Security Team: - Email: security@richesreach.com - Slack: #security-team - On-Call: PagerDuty rotation

Emergency Contacts: - Security Lead: [Name] - [Phone] - CTO: [Name] - [Phone] - Legal: [Name] - [Phone]

Next Review Date: [Quarterly]
Last Updated: 2026-01-XX
Version: 1.0