HOACart.AI Security Incident Response Plan

Document Version: 1.0
Effective Date: February 2026
Last Review Date: February 2026
Next Review Date: August 2026
Document Owner: Security Team
Classification: Internal Use

---

1. Purpose & Scope

This Security Incident Response Plan (SIRP) establishes procedures for detecting, responding to, and recovering from security incidents affecting HOACart.AI and its customers' data. This plan applies to all HOACart.AI systems, personnel, and third-party partners with access to our infrastructure.

1.1 Objectives

- Minimize impact and damage from security incidents
- Ensure rapid detection and containment
- Preserve evidence for investigation
- Maintain regulatory compliance (CCPA, state AI transparency laws)
- Restore normal operations efficiently
- Prevent recurrence through lessons learned

1.2 Covered Incident Types

- Unauthorized access to systems or data
- Data breaches (confirmed or suspected)
- Malware infections
- Denial of service attacks
- Insider threats
- Social engineering attacks
- Physical security breaches
- AI/ML system manipulation

---

2. Incident Classification

2.1 Severity Levels

Severity	Description	Response Time	Examples
CRITICAL	Active breach with data exfiltration	Immediate (< 15 min)	Confirmed data breach, ransomware, active attacker
HIGH	Significant threat with potential data exposure	< 1 hour	Brute force attack success, privileged account compromise
MEDIUM	Contained threat requiring investigation	< 4 hours	Multiple failed logins, suspicious API usage
LOW	Minor security event for monitoring	< 24 hours	Policy violation, single failed login attempt

2.2 Incident Categories

1. **Authentication Incidents**
   - Brute force attacks
   - Credential stuffing
   - Session hijacking
   - Account takeover

2. **Data Incidents**
   - Unauthorized data access
   - Data exfiltration
   - Mass data export
   - Sensitive data exposure

3. **Application Incidents**
   - SQL injection attempts
   - XSS attacks
   - API abuse
   - Privilege escalation

4. **Infrastructure Incidents**
   - DDoS attacks
   - Malware detection
   - Unauthorized system access
   - Configuration changes

---

3. Detection Methods

HOACart.AI employs multiple layers of detection:

3.1 Automated Detection

Detection Type	Trigger Threshold	Alert Severity
Brute Force	5+ failed logins in 5 min from same IP	HIGH
Credential Stuffing	10+ IPs with 3+ failures each in 30 min	HIGH
Session Hijacking	3+ IPs for same session in 5 min	HIGH
Mass Data Export	100+ records exported in single request	HIGH
SQL Injection	Pattern match on input	HIGH
XSS Attempt	Script pattern in input	MEDIUM
Unusual Access	Off-hours access (2-5 AM UTC) without history	MEDIUM
Rate Limiting	100+ requests/min from single IP	MEDIUM

3.2 Manual Detection Sources

- User reports via support@hoacart.ai
- Third-party security researchers
- Routine security audits
- Penetration testing results
- Law enforcement notifications

3.3 Monitoring Dashboard

Security incidents are tracked via `/admin/monitoring` with:
- Real-time alert feed
- 24-hour trend analysis
- Active incident count
- Threat level indicator

---

4. Incident Response Team (IRT)

4.1 Team Structure

Role	Responsibilities	Contact
Incident Commander	Overall coordination, decision authority	security@hoacart.ai
Technical Lead	Technical analysis, containment, remediation	engineering@hoacart.ai
Communications Lead	Internal/external communications, notifications	communications@hoacart.ai
Legal/Compliance	Regulatory requirements, legal guidance	legal@hoacart.ai
Executive Sponsor	Resource authorization, escalation	executive@hoacart.ai

4.2 Escalation Matrix

```
LOW → Technical Lead → Review within 24 hours
MEDIUM → Technical Lead → Incident Commander notification → 4-hour response
HIGH → Incident Commander → Executive Sponsor notification → 1-hour response
CRITICAL → Full IRT activation → Immediate all-hands → 15-minute response
```

---

5. Response Phases

Phase 1: Detection & Identification (0-15 minutes)

Objectives: Confirm incident, assess severity, activate response

Actions:
1. Receive and acknowledge alert
2. Verify incident is real (not false positive)
3. Classify severity level
4. Document initial findings:
- Time of detection
- Detection source
- Affected systems
- Initial indicators of compromise (IOCs)
5. Activate appropriate IRT members
6. Begin incident log

Checklist:
- [ ] Alert received and acknowledged
- [ ] Incident verified

- [ ] Severity classified
- [ ] Incident log started
- [ ] IRT notified

Phase 2: Containment (15-60 minutes)

Objectives: Stop the spread, preserve evidence, limit damage

Short-term Containment:
1. Isolate affected systems (if necessary)
2. Block malicious IPs/accounts
3. Revoke compromised credentials
4. Disable compromised features
5. Preserve system state for forensics

Long-term Containment:
1. Apply temporary fixes
2. Implement additional monitoring
3. Prepare clean systems for recovery

Checklist:
- [ ] Threat isolated
- [ ] Malicious actors blocked
- [ ] Credentials rotated
- [ ] Evidence preserved
- [ ] Backup systems ready

Phase 3: Eradication (1-24 hours)

Objectives: Remove threat, identify root cause

Actions:
1. Identify and remove malware/backdoors
2. Patch vulnerabilities exploited
3. Update security configurations
4. Reset all potentially compromised credentials
5. Review access logs for lateral movement
6. Document root cause analysis

Checklist:
- [ ] All malicious artifacts removed
- [ ] Vulnerabilities patched
- [ ] Credentials reset
- [ ] Root cause identified
- [ ] Documentation updated

Phase 4: Recovery (24-72 hours)

Objectives: Restore normal operations safely

Actions:
1. Restore systems from clean backups (if needed)
2. Gradually bring systems back online
3. Monitor closely for signs of recurrence
4. Verify data integrity
5. Test security controls
6. Return to normal operations

Checklist:
- [ ] Systems restored
- [ ] Monitoring verified
- [ ] Data integrity confirmed
- [ ] Security controls tested
- [ ] Normal operations resumed

Phase 5: Post-Incident Review (Within 7 days)

Objectives: Learn and improve

Actions:
1. Conduct post-mortem meeting
2. Document timeline of events
3. Identify what worked and what didn’t
4. Update incident response procedures
5. Implement additional preventive measures
6. Brief stakeholders on lessons learned

Deliverables:
- Post-Incident Report
- Updated detection rules
- Improved response procedures
- Training recommendations

---

6. Communication Procedures

6.1 Internal Communications

Audience	Channel	Timing
IRT	Dedicated Slack channel	Immediate
Engineering	#engineering Slack	After containment
Leadership	Email + meeting	Within 1 hour (CRITICAL)
All Staff	Email	After initial assessment

6.2 External Communications

Customer Notification Requirements:
- Within 72 hours of confirmed data breach (per CCPA and state laws)
- Include: Nature of incident, data affected, remediation steps, support contact

Regulatory Notifications:
- California AG (CCPA) - within 72 hours if > 500 CA residents affected
- Florida (SB 822) - within 30 days if financial data affected
- Law enforcement - as required by severity

Template locations:
- `/templates/security-incident-customer-notice.md`
- `/templates/security-incident-regulatory-notice.md`

6.3 Media/Public Communications

- All external communications approved by Communications Lead
- Prepared holding statement available
- Single spokesperson designated

---

7. Documentation Requirements

7.1 Incident Log

Maintain throughout incident:
- Timestamps for all actions
- Personnel involved
- Decisions made and rationale
- Evidence collected
- Communications sent

7.2 Evidence Preservation

- System logs
- Network traffic captures
- Memory dumps (if applicable)
- Configuration snapshots
- User activity logs

7.3 Post-Incident Report

Required elements:
1. Executive summary
2. Timeline of events
3. Root cause analysis
4. Impact assessment
5. Response evaluation
6. Recommendations
7. Appendices (logs, evidence)

---

8. Compliance Considerations

8.1 State-Specific Requirements

California (CCPA):
- Notify within 72 hours of confirmed breach
- Include specific elements in notification
- Provide free credit monitoring if SSN exposed

Florida (SB 822 & SB 908):
- Digital portal security requirements
- Financial data protection mandates
- CAM licensing compliance

New York (SB S8420A):
- AI decision audit requirements
- Disclosure of AI involvement in decisions

Washington (HB 2481):
- AI transparency requirements
- Anti-discrimination in automated decisions

8.2 AI-Related Incidents

For incidents involving AI/ML systems:
- Review AI Audit Log for affected decisions
- Assess if tenant challenges required
- Document human review of AI decisions
- Notify affected individuals of AI involvement

---

9. Testing & Maintenance

9.1 Plan Testing

- **Tabletop exercises:** Quarterly
- **Technical drills:** Semi-annually
- **Full simulation:** Annually

9.2 Plan Updates

- Review after every significant incident
- Scheduled review: Every 6 months
- Update after major system changes
- Update for new regulatory requirements

---

10. Appendices

Appendix A: Contact Information

[Maintain separate secure document]

Appendix B: System Inventory

- HOACart.AI Web Application
- PostgreSQL Database
- AWS Infrastructure (S3, etc.)
- Third-party integrations (Stripe, QuickBooks)

Appendix C: Detection Rule Reference

See `/lib/monitoring-service.ts` for automated detection thresholds.

Appendix D: Response Checklists

[See Phase sections above]

Document Control

Version	Date	Author	Changes
1.0	Feb 2026	Security Team	Initial release
