# Security Incident Response Plan

**Document ID:** IT-SEC-020 **Last Updated:** 2024-01-25 **Owner:** Security Team **Classification:** Internal

## Overview

This document outlines NovaTech's procedures for responding to security incidents. Rapid, coordinated response minimizes damage and ensures proper handling of security events.

## Incident Classification

### Severity Levels

| Level | Definition | Examples | Response Time |
|---|---|---|---|
| Critical (P1) | Active breach, data exfiltration, system compromise | Ransomware, active attacker, customer data breach | Immediate |
| High (P2) | Significant threat, potential breach | Detected malware, compromised credentials, phishing success | 1 hour |
| Medium (P3) | Security concern, limited impact | Failed attack attempts, policy violations, minor vulnerability | 4 hours |
| Low (P4) | Informational, minimal risk | Security questions, suspicious but benign activity | 24 hours |

## Incident Response Team

### Core Team

| Role | Primary | Backup | Contact |
|---|---|---|---|
| Incident Commander | CISO | Security Lead | security@novatech.com |
| Technical Lead | Sr. Security Engineer | Platform Lead | #security-urgent |
| Communications Lead | VP Communications | PR Manager | comms@novatech.com |
| Legal Counsel | General Counsel | Outside Counsel | legal@novatech.com |

### Extended Team (as needed)

- Engineering leads
- IT Operations
- Customer Success
- HR (if employee-related)
- Executive team (P1 incidents)

---

## Response Phases

### Phase 1: Detection & Reporting

**Anyone who detects a potential incident should:** 1. Do not attempt to investigate or fix on your own 2. Report immediately via: - Slack: #security-urgent - Email: security@novatech.com - Phone: +1-512-555-0199 (critical)

**Include in report:** - What you observed - When it occurred - Systems/data potentially affected - Any actions you've taken

### Phase 2: Triage

Security team will: 1. Acknowledge report within 15 minutes 2. Assess severity level 3. Assign incident commander 4. Create incident channel (#incident-YYYY-MM-DD-name) 5. Begin documentation in incident tracker

### Phase 3: Containment

**Immediate containment (as appropriate):** - Isolate affected systems - Disable compromised accounts - Block malicious IPs/domains - Preserve evidence

**Short-term containment:** - Apply temporary fixes - Enhanced monitoring - Limit access to affected systems

### Phase 4: Eradication

- Remove malware/threats
- Patch vulnerabilities
- Reset compromised credentials
- Clean affected systems

### Phase 5: Recovery

- Restore systems from clean backups
- Verify system integrity
- Monitor for reoccurrence
- Gradual return to normal operations

### Phase 6: Post-Incident

- Conduct post-mortem within 72 hours
- Document lessons learned
- Update procedures as needed
- Implement preventive measures
- Close incident ticket

---

## Communication Protocols

### Internal Communication

**During incident:** - All communication in designated incident channel - Hourly updates minimum for P1/P2 - No discussion outside incident channel - Document all decisions

**Post-incident:** - Summary to affected teams - All-hands update for significant incidents - Training updates if needed

### External Communication

**Customer notification (if required):** - Legal review before any external communication - Follow data breach notification requirements - Coordinate with Customer Success - Prepared statement from Communications team

**Regulatory notification:** - GDPR: 72 hours for personal data breaches - Other regulations as applicable - Legal coordinates all regulatory communication

**Law enforcement:** - Only if criminal activity suspected - Legal must approve and coordinate - Preserve evidence appropriately

---

## Specific Incident Procedures

### Compromised Credentials

1. Immediately disable affected account(s)
2. Reset passwords and revoke sessions
3. Review account activity logs
4. Check for lateral movement
5. Notify affected user
6. Determine how compromise occurred
7. Implement additional controls

### Malware Detection

1. Isolate affected system (disconnect from network)
2. Do not power off (preserves memory)
3. Security team begins forensic analysis
4. Identify malware type and capabilities
5. Check for spread to other systems
6. Wipe and reimage affected systems
7. Restore from clean backup

### Phishing Attack

1. Block sender/domain
2. Remove emails from all mailboxes
3. Identify who clicked/submitted credentials
4. Reset passwords for affected users
5. Check for post-compromise activity
6. Update email filters
7. Send awareness reminder

### Data Breach

1. Identify data involved and scope
2. Stop ongoing exfiltration
3. Preserve evidence
4. Legal assessment of notification requirements
5. Prepare customer/regulatory notifications
6. Executive briefing
7. Long-term remediation plan

### Denial of Service (DoS/DDoS)

1. Activate DDoS mitigation (Cloudflare)
2. Identify attack vectors
3. Implement blocking rules
4. Scale infrastructure if needed
5. Coordinate with ISP if necessary
6. Monitor for data exfiltration (often a distraction)

---

## Evidence Handling

### Preservation

- Create forensic images before changes
- Document chain of custody
- Secure physical evidence
- Maintain access logs

### Documentation

- Timestamp all observations
- Screenshot suspicious activity
- Save logs before rotation
- Record all actions taken

### Legal Hold

- Triggered for significant incidents
- Suspend data deletion
- Preserve all relevant records

- Legal coordinates process

---

## Post-Incident Review

### Timeline

- Initial review: 24 hours after resolution
- Full post-mortem: Within 72 hours
- Final report: Within 2 weeks

### Post-Mortem Contents

1. Incident summary
2. Timeline of events
3. Root cause analysis
4. Impact assessment
5. Response evaluation
6. Lessons learned
7. Action items with owners

### Action Item Tracking

- All items logged in tracking system
- Assigned owners and due dates
- Reviewed in weekly security meeting
- Escalated if overdue

---

## Training & Exercises

### Regular Training

- Annual tabletop exercises
- Quarterly phishing simulations
- New hire incident response training

### Exercise Types

| Exercise | Frequency | Participants |
|---|---|---|
| Tabletop | Annual | IRT + leadership |
| Simulation | Quarterly | Security team |
| Full drill | Annual | Company-wide |

---

## Contact Information

### Emergency Contacts

- Security Hotline: +1-512-555-0199 (24/7)
- Security Email: security@novatech.com
- Slack: #security-urgent
- On-call: PagerDuty "Security On-Call"

### External Resources

- Legal (external): [Outside Counsel Contact]
- Forensics partner: [Forensics Firm Contact]
- Insurance: [Cyber Insurance Carrier]
- FBI Cyber: ic3.gov

---

*Related Documents: Security Best Practices (IT-SEC-010), Data Classification Policy (COM-DP-001), Business Continuity Plan (IT-OPS-050)*