Incident Management Process

Document ID: IT-SUP-020 **Last Updated:** March 2024 **Owner:** IT Operations **Applies To:** All Technical Teams

---

Overview

This document defines NovaTech's incident management process for detecting, responding to, and resolving service disruptions. Effective incident management minimizes impact to customers and business operations.

Incident Definition

An incident is any unplanned interruption to an IT service or reduction in the quality of an IT service that affects users or business operations.

Examples

- Service outage (partial or complete)
- Performance degradation
- Security breach or threat
- Data loss or corruption
- System malfunction
- Integration failure

Incident Severity Levels

Severity	Definition	Examples	Response
P1 - Critical	Complete service outage affecting all users or data breach	Production down, security incident, data loss	Immediate, 24/7

Severity	Definition	Examples	Response
P2 - High	Major functionality impaired for many users	Key feature unavailable, severe performance degradation	<15 minutes
P3 - Medium	Limited impact, workaround available	Minor feature broken, moderate slowness	<1 hour
P4 - Low	Minimal impact, cosmetic issues	UI glitch, minor inconvenience	<4 hours

---

Incident Lifecycle

```
 Detection     Triage      Response     Resolution    Review
```

1. Detection

Incidents are detected through: - **Automated monitoring** - Alerts from DataLens, PagerDuty - **User reports** - Support tickets, Slack messages - **Internal reports** - Employee observations - **External reports** - Customer communications

2. Triage

- Assess severity and impact
- Assign incident commander (P1/P2)
- Create incident channel
- Notify stakeholders

3. Response

- Investigate root cause
- Implement mitigation
- Communicate status
- Escalate if needed

4. Resolution

- Confirm service restored
- Verify no side effects
- Update stakeholders
- Close incident

5. Review

- Conduct post-mortem (P1/P2)
- Document lessons learned
- Create action items
- Update runbooks

Roles and Responsibilities

Incident Commander (IC)

Required for P1/P2 incidents: - Coordinates response activities - Makes decisions on response actions - Manages communication - Declares incident resolved

On-Call Engineer

- First responder to alerts
- Initial triage and investigation
- Implements fixes or mitigations
- Escalates when needed

Subject Matter Expert (SME)

- Provides domain expertise
- Assists with diagnosis
- Recommends solutions

Communications Lead

For P1 incidents: - Manages external communication - Updates status page - Coordinates customer notification

Scribe

For P1/P2 incidents: - Documents timeline - Records actions taken - Captures decisions

---

Incident Response Process

P1/P2 Incidents

1. **Acknowledge alert** within 5 minutes
2. **Create incident channel** in Slack: `#inc-YYYYMMDD-description`
3. **Page incident commander** if not auto-assigned
4. **Assess and declare severity**
5. **Assemble response team**
6. **Begin investigation and mitigation**
7. **Provide regular updates** (every 15-30 minutes)
8. **Update status page**
9. **Declare resolved** when service restored
10. **Schedule post-mortem** within 48 hours

P3/P4 Incidents

1. **Acknowledge alert** or ticket
2. **Investigate and resolve**
3. **Document resolution** in ticket
4. **Close incident**

Communication

Internal Communication

Audience	P1	P2	P3/P4
Engineering	Slack channel	Slack channel	Ticket
Leadership	Slack + email	Slack	-
All company	Major incidents only	-	-

External Communication

Audience	P1	P2	P3/P4
Status page	Yes	Yes	If visible
Affected customers	Direct + status	Status page	If requested
All customers	Major incidents	-	-

Status Page Updates

Update **status.novatech.com** for customer-visible issues:

1. **Investigating** - Aware of issue, investigating
2. **Identified** - Root cause found, working on fix
3. **Monitoring** - Fix deployed, monitoring
4. **Resolved** - Issue resolved

Example update: > “We are experiencing degraded performance in the US-West region. Our team is actively investigating. Updates will be provided every 30 minutes.”

Escalation

Escalation Triggers

Escalate when: - Unable to resolve within expected timeframe - Impact is expanding - Additional expertise needed - Customer escalation received - Regulatory or legal implications

Escalation Path

```
On-Call Engineer


Engineering Manager (P3+)


Director of Engineering (P2+)
```

```
VP Engineering (P1)


CTO (Critical P1)
```

Escalation Contact Methods

Role	Primary	Secondary
On-call	PagerDuty	Slack
Manager	PagerDuty	Phone
Director	Phone	Email
VP+	Phone	-

On-Call

On-Call Rotation

- **Primary on-call**: First responder
- **Secondary on-call**: Backup/escalation
- **Rotation**: Weekly, handoff on Monday 9 AM CT

On-Call Expectations

- Respond to pages within 5 minutes
- Have laptop and internet access
- Remain able to work for duration
- Escalate if unavailable

On-Call Compensation

- Additional pay per on-call shift
- Time off for extended incidents
- See HR policy for details

Tools

Monitoring & Alerting

Tool	Purpose
DataLens	Metrics, dashboards
PagerDuty	Alert routing, on-call
Slack	Communication
Status page	Customer communication

Incident Management

Tool	Purpose
Jira	Incident tracking
Confluence	Runbooks, documentation
Google Docs	Post-mortem documents

Runbooks

Runbook Requirements

Every service must have runbooks covering: - Service overview - Dependencies - Common issues and fixes - Escalation contacts - Monitoring and alerts

Runbook Location

Runbooks stored in Confluence: `Engineering → Runbooks → [Service Name]`

Runbook Template

```
# Service Name Runbook

## Overview
Brief description of the service

## Dependencies
- List of dependent services
- External dependencies

## Common Issues

### Issue: High latency
**Symptoms:** Response time > 500ms
**Causes:** Database load, cache miss
**Resolution:**
1. Check database metrics
2. Verify cache hit rate
3. Scale if needed

### Issue: Service unavailable
...

## Contacts
- Team: #team-channel
- On-call: PagerDuty
- Escalation: Manager name
```

Post-Mortem Process

When Required

Post-mortems are required for: - All P1 incidents - All P2 incidents - Recurring P3 incidents - Customer-escalated incidents

Timeline

- **48 hours**: Schedule post-mortem meeting
- **5 business days**: Complete post-mortem document
- **2 weeks**: Complete action items or have plan

Post-Mortem Document

Include: 1. **Summary** - Brief description 2. **Impact** - Duration, users affected, business impact 3. **Timeline** - Detailed sequence of events 4. **Root cause** - Why did this happen? 5. **What went well** - Effective response actions 6. **What could improve** - Process gaps 7. **Action items** - Specific, assigned improvements

Post-Mortem Principles

- **Blameless** - Focus on systems, not individuals
- **Learning-focused** - Goal is improvement
- **Action-oriented** - Every incident drives improvement
- **Thorough** - Dig deep into root causes

Metrics

Key Metrics

Metric	Target
MTTA (Mean Time to Acknowledge)	P1: <5 min, P2: <15 min
MTTR (Mean Time to Resolve)	P1: <1 hour, P2: <4 hours
Incident volume	Trending down
Post-mortem completion	100% for P1/P2
Action item completion	>90% within 2 weeks

Reporting

- Weekly incident summary
- Monthly incident review
- Quarterly trend analysis

Training

Required Training

- On-call onboarding
- Incident commander training
- Service-specific runbook review

Exercises

- Monthly incident response drill
- Quarterly disaster recovery test
- Annual chaos engineering exercise

Related Documents

- On-Call Policy (IT-SUP-025)
- Change Management (IT-OPS-015)
- Security Incident Response (IT-SEC-020)
- Disaster Recovery Plan (IT-OPS-030)

Contact

- **IT Operations:** it-ops@novatech.com
- **Security incidents:** security@novatech.com
- **Slack:** #incident-response

Review Cycle: Quarterly Next Review: June 2024