

## Standard Operating Procedure

### SOP-IT-009: Incident Response

<b>Document ID:</b>	SOP-IT-009	<b>Version:</b>	1.0
<b>Effective Date:</b>	YYYY-MM-DD	<b>Review Date:</b>	YYYY-MM-DD

#### 1. Purpose

This SOP defines the technical response procedures for IT security incidents and system failures.

#### 2. Scope

This SOP applies to all IT security incidents, system outages, and technical emergencies.

#### 3. Incident Response Phases

##### Phase 1: Detection & Analysis

- Automated monitoring alerts (CloudWatch, Datadog)
- User reports via GitHub Issues or Slack
- Initial triage by SRE on-call

##### Phase 2: Containment

- Isolate affected systems
- Preserve evidence (logs, snapshots)
- Activate incident response team if P1

##### Phase 3: Eradication & Recovery

- Root cause identification
- Apply fixes via emergency change process
- Restore services from backups if needed

##### Phase 4: Post-Incident

- Post-mortem report (within 48 hours)
- CAPA if quality impact (SOP-IT-005)
- Update runbooks and monitoring

#### 4. Communication Protocol

- P1 incidents: Notify Quality Manager within 1 hour
- Status updates: Every 2 hours during active incident

- All stakeholder communication via Slack #incidents channel

#### 5. Documentation Requirements

- **Incident timeline with timestamps**
- Actions taken and by whom
- Root cause analysis
- Lessons learned and preventive measures

#### 6. Approvals

This document requires electronic signature approval via DocuSign (21 CFR Part 11 compliant).

<b>Role</b>	<b>Name</b>	<b>Signature &amp; Date</b>
Author	[Name]	[DocuSign]
Reviewer (QA Lead)	[Name]	[DocuSign]
Approver (Quality Manager)	[Name]	[DocuSign]