IT Incident Response Procedure

Incident Classification

Incidents are classified by severity: P1 (Critical - system down), P2 (High - major functionality impaired), P3 (Medium - minor impact), P4 (Low - minimal impact).

Response time SLAs: P1 - 15 minutes, P2 - 1 hour, P3 - 4 hours, P4 - next business day. Escalation occurs if SLAs are not met.

Incident Detection and Reporting

Incidents may be detected through monitoring alerts, user reports, or security scans. Report incidents via IT helpdesk portal, email, or phone.

Provide detailed information: what happened, when, who's affected, error messages, and steps to reproduce. Screenshots are helpful.

Initial Response

On-call engineer acknowledges incident and begins triage. Assess severity, impact, and urgency. Notify stakeholders if customer-facing systems are affected.

Create incident ticket with all relevant details. Begin investigation to identify root cause. Implement temporary workarounds if possible.

Escalation Procedures

Escalate to senior engineers or specialists if incident cannot be resolved within SLA timeframe or requires specialized expertise.

For P1 incidents, notify incident commander and assemble response team. Establish communication bridge for coordination.

Communication During Incidents

Post status updates in #incidents Slack channel every 30 minutes for P1/P2, hourly for P3. Update incident ticket with progress.

Notify affected users through status page. Provide estimated time to resolution when known. Be transparent about impact and progress.

Resolution and Recovery

Once root cause is identified, implement fix and verify resolution. Monitor systems to ensure stability. Document resolution steps.

Conduct post-incident review within 48 hours for P1/P2 incidents. Identify lessons learned and preventive actions.

Post-Incident Review

Review timeline, root cause, impact, and response effectiveness. Identify what went well and areas for improvement.

Create action items to prevent recurrence. Update runbooks and documentation. Share learnings with broader team.

Documentation Requirements

All incidents must be fully documented including timeline, actions taken, root cause, and resolution. Update knowledge base with solutions.

Maintain incident metrics for trend analysis and continuous improvement. Report major incidents to leadership.