Incident Response Runbook Template

A simple framework for managing cloud incidents effectively

1■■ Incident Overview

- Incident ID: _____
- Date & Time: _____
- Reported by: _____
- Service/System affected: _____
- Severity level (High/Medium/Low): _____

2■■ Incident Detection & Reporting

- ■ How was the incident detected? (Monitoring alert, user report, audit, etc.)
- ■ Who reported the incident?
- ■ Initial assessment or symptoms: _____

3■■ Communication Plan

- ■ Internal communication channel: (Slack, Teams, Email, etc.)
- ■ Stakeholders to be informed: _____
- ■ Customer notification needed? Yes / No

4■■ Incident Response Actions

- ■ Containment steps taken: _____
- ■ Root cause analysis started: Yes / No
- ■ Systems impacted: _____
- ■ Responsible team/person: _____

5■■ Recovery & Resolution

- ■ Steps taken to restore service: _____
- ■ Service restoration date/time: _____
- ■ Verification completed by: _____

6■■ Post-Incident Review

- ■ Lessons learned: _____
- ■ Preventive actions: _____

- ■ Follow-up ticket/plan created: Yes / No
- ■ Owner responsible: _____

7■■ Attachments

- Add screenshots, logs, and relevant documentation here.

■ **Tip:** Conduct a post-incident review after every major outage to continuously improve your cloud resilience.

■ Need help implementing? Contact: your.email@example.com