Incident response playbook template

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

Playbook header

Fill in once per playbook.

- Name: [incident type].
- Owner: [role]. Approved on [date]. Review every [12 months].
- Use when: [trigger in one sentence].
- Do not use when: [what belongs to another playbook].

Prerequisites

What must be in place before an incident.

- Logs to be on: [list].
- Access and roles responders need: [list].
- Tools and contacts: [list].

Workflow

Numbered steps in order. One action per step. Name the role.

1. [Step 1: action, role, expected result]
2. [Step 2]
3. [Step 3]

Decision points

Each point where a person must decide.

Decision	Who decides	Information needed	If yes	If no
[question]	[role]	[facts]	[next step]	[next step]

Checklist

A tick-list that mirrors the workflow, for regulated settings.

- [ ] [Step 1 done, time, by]
- [ ] [Step 2 done, time, by]

Exit criteria and follow-up

When to close and what to update.

- Exit when: [criteria].
- Update: [plan, detections, contacts].
- Review date: [date].