Blameless Postmortem — Incident Review Record

Incident ID: _____
Detected (date / time): _____
Resolved (date / time): _____
Severity: _____
Services affected: _____
Incident commander: _____
Author: _____
Review date: _____

1 — Summary

Two or three sentences someone outside the team can follow: what broke, for whom, for how long, and what ended it. No names.

2 — Impact

Users affected · failed requests · duration of degradation · SLA or revenue consequence · what customers actually saw. Numbers, not adjectives.

3 — Timeline

Every entry needs a source — an alert, a graph, a message. If you cannot say how you knew, it is a reconstruction, not a timeline.

Time (UTC)	Event	How we knew

4 — Detection

How it was detected: alert, customer report, someone noticing? Time from first impact to detection — often the biggest number in the record.

5 — Contributing factors

Conditions that all had to be true for this to happen. Systems, defaults, missing signals, decisions made with the information available at the time. Expect several, not one.

6 — What went well

Keep it — this is what you are trying not to lose in the next reorg.

7 — Where we got lucky

What worked this time but is not guaranteed to work again. The honest section, and the first one to get deleted.

8 — Action items

Type each action: prevent (stops the cause), detect (finds it sooner), mitigate (reduces the blast radius). A list of only 'prevent' items usually means the detection gap was not discussed.

Action	Type	Owner	Due	Ticket

9 — Follow-up

How you will know these actions worked · review date · what would reopen this postmortem.