

Production incident response

What the on-call engineer does in the first thirty minutes of a production incident, written to be followed with one hand.
If you are unsure of the severity, treat it as one level worse.

THIS RUNBOOK STARTS WHEN

A page fires, a customer reports an outage, or you see error rates above 2% for five minutes.

It ends when the incident is resolved in the channel and the timeline is written. Root cause, fixes and the postmortem happen after, under RB-INC-02.

1	Acknowledge the page Acknowledge in the pager, not in chat. An unacknowledged page escalates to the secondary after five minutes and to the duty manager after ten, which pulls three people out of bed instead of one.	Within 2 min On-call primary
2	Open the incident channel and say what you know One line is enough: what is broken, what you are looking at, and that you are the incident lead. Do not investigate before you have opened the channel — a silent twenty minutes is the thing every postmortem complains about.	Within 5 min Incident lead
3	Set a severity and say it out loud Use the table below. Severity drives who else wakes up, so it is a decision, not a guess: write it in the channel as SEV-2 declared with the time.	Within 5 min Incident lead
4	Stop the bleeding before you find the cause Roll back the last deploy, fail over the region, or turn the feature flag off. A five-minute rollback beats a thirty-minute diagnosis, and the cause will still be there in the morning.	Within 15 min Incident lead
5	Post an update every fifteen minutes Even when the update is “no change, still looking.” Support cannot answer customers from silence, and the status page is written from these updates.	Every 15 min Incident lead
6	Declare it resolved, then write the timeline Resolved means error rates are normal and have stayed normal for ten minutes. Write the timeline while it is fresh: first signal, first action, what worked. The postmortem is scheduled within two working days.	Same shift Incident lead

SEVERITY

LEVEL	MEANS	WAKES UP	UPDATE EVERY
SEV-1	Checkout or billing down for everyone	On-call, secondary, duty manager, VP eng	10 minutes
SEV-2	A major feature down, or one region degraded	On-call, secondary	15 minutes
SEV-3	Degraded but usable; a workaround exists	On-call only	30 minutes

ESCALATION LADDER

AFTER	ESCALATE TO	HOW	CONTACT
5 min	Secondary on-call	Pager escalates automatically	Rota page
15 min	Duty manager	Call, do not message; SEV-1 escalates at 5 minutes	+1 (415) 555-0198
30 min	VP engineering and support lead	Call, and post the status-page draft	Elena Marsh

Nobody here has been criticised for declaring an incident that turned out to be minor. The failure this runbook exists to prevent is the opposite: one engineer quietly working a problem for forty minutes while support answers customers with nothing. **Open the channel early and ask for help before you need it.**