Incident response and post-mortem

Manual | 12 steps | 3 roles | Created Sep 2, 2026 | Updated Sep 2, 2026 | v1

How an incident lead and on-call engineer triage, communicate, resolve, and learn from a service incident.

TRIGGER

When any team member observes a customer-affecting failure, or an automated alert fires for a service degradation.

12 STEPS

1 **The person who noticed the issue declares an incident in the agreed channel, stating what is broken and what they observed.**

Declaring early and being wrong is much cheaper than deliberating. Nobody should hesitate to declare because they are unsure it qualifies.

2 **Incident Lead takes ownership by name and states so explicitly in the channel.**

One named owner. An incident with no explicit owner has several people assuming someone else is coordinating.

3 **Incident Lead assesses severity based on customer impact.**

Assess by impact, not by how technically alarming the cause looks. A noisy internal failure with no customer effect is not a high-severity incident.

Customers affected or data at risk: Go to step 4: Communications Owner notifies affected customers with what is known, what is being done, and when the next update will come.
No customer impact: Go to step 6: Responder investigates and applies a mitigation to restore service, recording each action taken in the incident channel as it happens.

4 **Communications Owner notifies affected customers with what is known, what is being done, and when the next update will come.**

Within 30 minutes of severity assessment

Commit to a next-update time and meet it even when there is no progress. Silence during an incident is what damages trust, not the incident.

5 **Communications Owner posts updates at the promised interval until resolution.**

An update saying we are still investigating and will update again in an hour is a real update.

6 **Responder investigates and applies a mitigation to restore service, recording each action taken in the incident channel as it happens.**

Restore service first and find the root cause second. Record actions as you go, because reconstructing a timeline afterwards from memory is unreliable and the post-mortem depends on it.

7 **Incident Lead confirms service is restored and verifies it independently rather than assuming.**

> Service restored: Go to step 8: Communications Owner confirms resolution to affected customers.
> Not resolved: Go to step 6: Responder investigates and applies a mitigation to restore service, recording each action taken in the incident channel as it happens.

8 **Communications Owner confirms resolution to affected customers.**

9 **Incident Lead schedules a post-mortem within five working days, while the detail is still recoverable.**

Within five working days

> Any longer and the timeline gets fuzzy and the urgency evaporates.

10 **Incident Lead runs a blameless post-mortem producing a timeline, the contributing causes, and what made detection or recovery slower than it should have been.**

> Blameless in practice, not just in name. The moment a post-mortem assigns fault, people stop volunteering the information that makes it useful.

11 **Incident Lead records each agreed action with a named owner and a due date.**

> An action without an owner and a date is not an action. This is where most post-mortems quietly fail.

12 **Incident Lead updates or creates the procedures the incident revealed to be missing or wrong.**

This is the step that stops recurrence. If the incident happened because a recovery procedure did not exist, the post-mortem is not finished until it does.

Procedures updated and actions assigned: Ends the procedure

ROLES INVOLVED

Incident Lead | Responder | Communications Owner

REVIEW CADENCE

After every high-severity incident, and quarterly regardless. This procedure is the one most likely to have been improved by recent experience.

Name the person accountable for this procedure before you put it into use.

CHANGE THESE BEFORE YOU USE IT

- Define your own severity levels with concrete criteria in step 3, since 'customer impact' needs to mean something specific in your business.
- Set the notification window in step 4 to whatever your service commitments actually require.
- Name your real channels and status page. A procedure that says 'the agreed channel' is not followable at 2am.
- If you have regulatory breach-notification duties, add them explicitly with their statutory deadlines. This template does not cover them.

This is a free starting point from sendabrief.com, not compliance advice. It is written to be adapted.

Source: https://sendabrief.com/templates/incident-response-and-post-mortem