

COMPLIANCE & SECURITY · PLAYBOOK

Incident Response Playbook Template

For founders and operations leaders who need a clear, ready-to-use first-response sequence for security and operational incidents.

How to use this: Fill in your decision-makers and severity levels now, before an incident happens, and keep this playbook somewhere the whole team can find quickly.

Severity Levels

Define what separates a minor issue from a serious one for your business specifically.

Severity	Example	Who Must Be Involved	Response Time Target
Low	Single account issue, no data exposure		
Medium	Limited data exposure, contained quickly		
High	Customer data exposure, active compromise, major outage		

Step 1: Contain

- ☐ Identify and stop the immediate exposure (revoke credentials, disable integration, take system offline).
- ☐ Preserve evidence where possible before making changes (screenshots, logs, timestamps).
- ☐ Assign a single incident lead who makes decisions for the duration of the response.

Step 2: Assess

What systems or data are confirmed to be affected?

What is still unknown or unconfirmed at this point?

How many customers or accounts are potentially affected?

What is the current severity level based on the table above?

Step 3: Communicate

- ☐ Internal stakeholders are notified first, based on severity level.
- ☐ Only confirmed facts are communicated, with no speculation presented as fact.
- ☐ Affected customers are notified if their data or service was impacted, with a clear next-update time.
- ☐ Any contractual or regulatory notification requirements are checked and actioned.
- ☐ One person owns all external communication to avoid conflicting messages.

Step 4: Stabilise and Document

What was the root cause, to the best of current knowledge?

What actions were taken, in order, with timestamps?

What will be done differently to prevent recurrence?

Who needs to review this incident once it's resolved, and by when?

Post-Incident Review

- ☐ Timeline of the incident is documented while details are still fresh.
- ☐ Root cause and contributing factors are identified without assigning blame.
- ☐ Concrete follow-up actions are assigned to named owners with deadlines.
- ☐ This playbook is updated if the incident revealed a gap in the process itself.