Example Incident Response Runbook

1. Triage the incident

- Confirm impact, affected systems, and the first known event.
- Assign an incident commander and open a shared timeline.
- Preserve logs before making destructive changes.

Example Incident Response Runbook

2. Contain and communicate

- Prefer reversible containment while evidence is incomplete.
- Record each decision, owner, timestamp, and expected effect.
- Send short status updates on a predictable cadence.

Example Incident Response Runbook

3. Recover and learn

- Validate service health before declaring recovery.
- Track follow-up work with owners and due dates.
- Run a blameless review and update the runbook.