SaaS Downtime Response Checklist

A step-by-step action list for handling downtime incidents — companion to How to Handle Downtime in SaaS: A Step-by-Step Guide

Incident Details

Incident name / ID:

Date and time detected:

Severity level (SEV1-4):

Incident Commander:

Status page link:

Work through "Before an Incident" once, as a team, to confirm your baseline readiness — then revisit it quarterly. During a live incident, work through "During an Incident" in order. Complete "After an Incident" within 24-48 hours of resolution, while details are still fresh.

Phase 1: Before an Incident — Readiness

Confirm these are in place before you need them. Revisit this section every quarter or after any major infrastructure change.

Incident response plan

- [ ] Incident response plan is documented and shared with the full team
- [ ] Roles are assigned: Incident Commander, Technical Lead, Communication Lead, Customer Support Lead, Subject Matter Expert
- [ ] Escalation path is defined — who gets notified, and at what point (e.g. after 15, 30, 60 minutes unresolved)
- [ ] Communication templates are prepared for service degradation, partial outage, and full outage
- [ ] Templates are tailored for each audience: customers, internal stakeholders, partners

Monitoring and alerting

- [ ] Infrastructure monitoring is in place (servers, databases, network)
- [ ] Application performance monitoring (APM) is in place
- [ ] Thresholds are set for key metrics: response time, error rate, CPU usage, memory usage
- [ ] Alerts are routed to multiple channels: email, SMS, Slack (or equivalent)

Redundancy and failover

- [ ] Multiple servers are deployed across different locations
- [ ] Databases are replicated across multiple servers or availability zones
- [ ] Cloud redundancy features are enabled: multiple availability zones and regions
- [ ] Failover has been tested, not just configured

Phase 2: During an Incident — Response

Work through this section in order, from the moment an outage is detected to the moment it is resolved.

Acknowledge

- [ ] Publicly acknowledge the issue as soon as it's detected — don't wait for full diagnosis
- [ ] Post an initial update to the status page
- [ ] Post a brief update to social media channels (if customer-facing impact is broad)
- [ ] Send an email notification to affected customers, if the incident warrants it
- [ ] Provide an estimated time of resolution (ETR), even if it's a broad range

Update

- [ ] Update the status page and other channels on a set interval (e.g. every 30 minutes) until resolved
- [ ] Revise the ETR as the situation evolves — don't let it go stale
- [ ] Explain the cause in plain language customers can understand, as soon as it's known
- [ ] Avoid downplaying severity or making promises the team can't keep

Resolve

- [ ] Confirm the fix is stable before declaring resolution — watch for recurrence
- [ ] Post an "all clear" update to the status page and other channels
- [ ] Send a final resolution notice to affected customers

Apologize and compensate

- [ ] Apologize clearly, without excuses or deflecting blame
- [ ] Determine compensation based on severity and duration — service credit, discount, extended trial, or other
- [ ] Communicate the compensation directly to affected customers

Phase 3: After an Incident — Review

Complete within 24-48 hours of resolution, while the details are still fresh for everyone involved.

Root cause analysis

- [ ] Gather logs, metrics, and monitoring data from the incident window
- [ ] Interview team members involved in the response for their perspective
- [ ] Review customer feedback and support tickets related to the incident

- [ ] Build a timeline of events leading up to and during the outage
- [ ] Identify the root cause(s) — avoid stopping at the first plausible explanation
- [ ] Document contributing factors separately from the root cause

Corrective action

- [ ] Write recommended corrective actions, each with a clear owner and deadline
- [ ] Update monitoring, alerting, or redundancy based on what the RCA revealed
- [ ] Update the incident response plan itself with any lessons learned

Close the loop

- [ ] Present the RCA to the internal team and discuss lessons learned openly
- [ ] Publish an external summary on the status page or blog, if the incident was customer-facing
- [ ] Thank customers for their patience in the external summary
- [ ] Confirm all corrective actions are tracked to completion, not just written down

Post-Incident Summary

Root cause (one sentence):

Total downtime duration:

Customers affected (number or %):

Compensation offered:

Corrective actions owner(s):

Target completion date for fixes: