

Website incident report: replace this template text with the short, plain-language title for the incident

© KevTom Consulting - V1.0 - November, 2025 - [public domain under CC0](#)

About the template: Copied from [source](#).
Use **File** → **Make a copy** to edit for your project or organization.

| INCIDENT KEY DETAILS | |
|---|---|
| Reported by <i>Name and contact</i> | Replace this text with the reporter's full name, department, email address and phone number. |
| Owner <i>Name and contact</i> | Replace this text with the incident owner or primary responder's full name, department, email address and phone number, if different from the reporter. |
| Date and time detected | Nov 14, 2025 12:00 PM - Change date and time to when the incident was detected or reported. Information about the exact time of occurrence goes here. |
| Date and time resolved | Nov 14, 2025 12:00 PM - Change date and time to when the incident was resolved, or mark PENDING. |
| Date of report <i>Creation date</i> | Nov 14, 2025 - Change date to the date this report is created. |
| Systems affected | Replace this text with the main website, app, CMS, API or service impacted. |
| Duration | Replace this text with the downtime duration of the incident |
| Demo URLs | Replace this text with the URLs of pages affected by the incident, if appropriate. |
| Related ticket(s) <i>Paste URLs</i> | Replace this text with links to bug, incident or development tickets. |
| Monitoring alert <i>Paste URL</i> | For use with a monitoring system such as PagerDuty, Datadog, Pingdom, etc. Replace this text with a direct link to the monitoring incident, if generated. |
| Severity <i>Choose one</i> | Level 1 Level 2 Level 3 Severity levels are detailed below. |
| Communication <i>Optional</i> | Replace this text with a link to any status page, internal or public notice. |

Incident summary

Replace this text with a brief, factual overview of what happened and the current status.

Detailed timeline

Nov 14, 2025 12:00 PM - Replace this text with a chronological log of events from detection through resolution.

Nov 14, 2025 12:00 PM - Replace this text with a chronological log of events from detection through

resolution.

Detection and escalation

Replace this text with how the incident was discovered and how it was escalated.

Impact assessment

Replace this text with the effect on users, systems, data and business operations, and highlight internal-only vs. customer-facing impacts.

Immediate response and containment

Replace this text with actions taken to stabilize and contain the incident.

Root cause analysis

Replace this text with the confirmed cause and contributing factors, if known.

Resolution and recovery

Replace this text with the final fix and how full service was restored.

Corrective and preventive actions

Replace this text with changes planned to prevent recurrence, including owners and timelines.

Evidence and references

Replace this text with links to logs, screenshots, tickets and supporting files.

Regulatory concerns

Replace this text with any notes about uptime SLAs or reporting obligations.

Lessons learned

Replace this text with any notes about what we have learned from the incident and response.

Post-incident review and approval

Reviewed by: Add reviewer names, dates and final sign-off notes, Nov 14, 2025



Severity levels

Edit the following default text to reflect the incident levels policy of your organization, and any required or suggested escalations, actions, notifications, responses or mitigations.

Level 1 Critical

Complete outage or major data loss. Core site, app or API is unavailable for most users. Immediate response required. Executive and communications teams may need to be notified.

Suggested or required action: Replace with immediate containment, rollback, failover or emergency mitigation steps, as dictated by organization policy.

Suggested or required contact(s): Replace with CEO, COO, CTO, CISO, legal, communications or on-call engineering leadership, as dictated by organization policy.

Level 2 High

Partial outage or severe functional degradation. Key features are broken but limited service remains available. Rapid response required. Stakeholders probably need to be notified.

Suggested or required action: Replace with prioritized investigation, hotfix, traffic routing or feature disablement, as dictated by organization policy.

Suggested or required contact(s): Replace with product owner, engineering manager, stakeholder leads and on-call support, as dictated by organization policy.

Level 3 Moderate

Minor service disruption, performance issue or non-critical bug. Limited user impact. Can be handled during normal operating hours. Notifications may be optional.

Suggested or required action: Replace with standard bug triage, backlog entry or scheduled maintenance fix, as dictated by organization policy.

Suggested or required contact(s): Replace with direct supervisor, team lead or assigned developer, as dictated by organization policy.



How to write an incident report

Edit the following default text to reflect the policy, style and brand of your organization.
Use this guide to ensure reports are clear, factual and useful for review and prevention.

Be objective

Write in plain, neutral language. Record facts only. Do not assign blame or speculate.

Write chronologically

Document events in the order they occurred, with timestamps where possible.

Be specific

Use exact system names, URLs, error messages and measurable impact.

Separate facts from analysis

Record impact and actions separately from confirmed root cause.

Document actions in real time

Log containment and recovery steps as they occur, not from memory.

Use full identification

List full names and roles for people and full names for systems on first reference.

Include evidence

Link directly to logs, alerts, tickets, screenshots and related files.

Document communications

Record who was notified, when and how. Link to any status updates.

Avoid hindsight bias

Record what was known at the time decisions were made.

Review for accuracy

Verify dates, times, actions and links before final submission.

