*Keep in mind **this is not a "template" it is a guide,** we expect that the usage of this will vary in terms of detail under certain headlines or use of certain headlines at all. Use your best judgment and include things that you feel are relevant.*

EVENT # (link to parent ticket): Short Description of Incident

How We Got Here

Investigators/Authors	*To remove bias, this should be someone who was **not** involved in incident mitigation or resolution.*
Incident Responders	*Include initial incident commander, closing incident commander, who spent the most time on this incident, which teams were involved, etc.*
Interviews	*Names of the folks interviewed.*

Narrative Description

This section should serve as a summary of what happened. Someone that is just scanning this document should be able to get a summary of this information here.

Event

2-3 sentence description of the anomalous (deviating from what is normal or expected) event.

jeli

Customer/Employee Impact (if any)

Where? How much? Who was impacted? In what way? Which KPI was impacted? (If there was a UI interaction involved here, screenshots are helpful!)

Trigger

The trigger is typically innocuous (not harmful on its own), and makes the vulnerabilities (from contributors/enablers) combine and lead to an event. Ex: The 'rollback button was pushed and several users couldn't access their workspaces'. In this example, pressing the rollback button would be the trigger, but pressing the rollback button on its own, wouldn't be something that is typically a vulnerability.

Key Takeaways/Themes/Questions

If someone was looking at this document a year or two from now. What would you want them to come away with? What stood out as important to discuss?

Contributors/Enablers

Think of these as things that had to be true for the incident to occur. Do not think of these as "causes" or people involved. Contributors and enablers create vulnerabilities that have remained latent in the system (sometimes for long periods of time!).

Risks

Did the incident reveal any risks in system or component design or highlight that the risks are more severe than we anticipated?

Mitigators

What did we do to fix the anomaly? What went well in the system? What went well in the moment? This can include: things that were already baked into the system, actions taken, how were they decided, people being available, processes working, etc.

Difficulties during handling

What happened in the moment of triaging that made things more difficult? Were people easy to get a hold of? Did people know who to page? Did people paged know what to do?

Were roles clear, of who was doing what? Was anyone brought in that wasn't explicitly on-call? If so, why did we need this particular person?

Follow-up Items

Link out to follow-up tracking tickets. The investigator should note if these follow-up items are about recovery or about prevention.

Resources

Any other things that relate to this incident: docs, Slack conversations outside of the incident channel, related PRs, other relevant incidents, other 'how we got here' docs, etc.

Timeline