Post-Incident Review

Goals:

We are here to **learn** the following:

1. How do we know sooner (*Detection*)?
2. How do we recover sooner (*Response & Remediation*)?

Key Metrics

Time to Acknowledge:_____

Time to Recover:_____

Elapsed Time of the Following Phases:

Detection:_____

Response:_____

Remediation:_____

Severity:_____

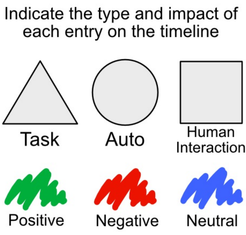
Customer Impacted (Yes/No):_____

Incident Commander *(optional)*:_____

Timeline

TIP: Describe rather than Explain

Suggested timeline data to capture:
- Date & Time of detection
- Date & Time of service restoration
- Incident Number (optional)*
- Who was paged first
- When was the incident acknowledged
- Who else was brought in to help and what time?
- Who was the acting Incident Commander (optional)?
- What tasks were performed and at what time?
- Which tasks made a positive impact to restoring service?
- Which tasks made a negative impact to restoring service?
- Which tasks made no impact to restoring service.
- Who executed specific tasks?
- What conversations were being had?
- What information was shared?



Time:	EngID:	Task:	Detail:
Example data:			
00:15:05			Incident #24 created (High CPU usage)
00:15:07	01		Eng01 "ack" incident #24
00:15:08	01		Eng01 contacts Eng02 for assistance

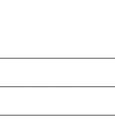
What does it look like when this goes well?

How can we improve?

_____ .. continue in additional space

Tasks and their impact on restoring service

Plot the tasks, human interactions, and automation along a timeline marking the impact on restoring service (good, bad, neutral). Noting the time between the phases of detection, response, and remediation, new target conditions can be established *(e.g. acknowledge incidents 50% faster)*.



Learnings

What have we learned by discussing the timeline? What new information was gained?

_____ .. continue in additional space

Action Items

Task ID: Owner:

_____ .. continue in additional space

Contributing Factors

_____ .. continue in additional space