# Incident Response Plan

* **Initial Alert Notification:**
  + When an alert is triggered in Grafana or CloudWatch, the first step is to notify the designated shift person or on-call responder immediately.
  + The notification can be sent via email, SMS, or a dedicated alerting platform like PagerDuty.
* **Incident Triage:**
  + Upon receiving the alert, the on-call responder acknowledges the alert and begins triaging the incident.
  + The responder verifies the nature and severity of the alert (with help of defined SLA’s and SLO’s) and determines whether it requires immediate action or can be handled during regular business hours.
  + If there’s greater business impact, the bridges are called with respective team.
* **Investigation and Root Cause Analysis:**
  + The responder investigates the root cause of the alert by accessing relevant monitoring tools such as Grafana and CloudWatch.
  + In Grafana, the responder examines application status dashboards to identify any anomalies or issues with the "Hello World" application.
  + In CloudWatch, the responder reviews EC2 metrics like CPU and memory usage to understand the system's overall health and performance.
  + The responder analyzes recent logs for the errors and the changes to the application or infrastructure that may have contributed to the alert.
* **Mitigation and Remediation:**
  + Based on the findings from the investigation, the responder takes appropriate actions to mitigate the alert and restore normal operation.
  + This may involve restarting the application server, scaling up resources (e.g., increasing EC2 instance size), or rolling back recent changes to the application or infrastructure.
  + The responder documents the steps taken during the incident response process for future reference and analysis. (Handy Runbooks)
* **Communication and Collaboration:**
  + Throughout the incident response process, the responder communicates updates and progress to relevant stakeholders, including team members, management, and customers (if applicable).
  + Regular status updates are provided via team chat channels, email, or a dedicated incident communication platform.
  + Collaboration tools like Slack or Microsoft Teams may be used to facilitate communication and coordination among team members.
* **Post-Incident Review and Analysis:**
  + After the incident has been resolved, a post-incident review (PIR) meeting is conducted to analyze the incident in detail.
  + The team reviews the timeline of events, root cause analysis, actions taken, and lessons learned from the incident.
  + Recommendations for preventing similar incidents in the future are discussed, and any necessary changes to processes, procedures, or infrastructure are implemented.
* **Documentation and Knowledge Sharing:**
  + The details of the incident, including its timeline, root cause analysis, and remediation steps, are documented in a incident management system.
  + This documentation serves as a reference for future incidents and helps improve incident response processes over time.
  + Key insights and lessons learned from the incident are shared with the broader team through post-incident reports or knowledge-sharing sessions.