# [Draft]Incident Response Plan

**2023-08 @Guzhongren**

# Agenda

- Definition of Incident
- Incident Severity
- Pre-Actions for the Incident
- Incident Response
- Post Actions of the Incident
- Q&A

# Definition of Incident

# What

- Definition of Incident

# Incident Severity

# Incident Severity

| Severity | Characteristics | Examples |
| --- | --- | --- |
| Critical | | |
| High | | |
| Medium | | |
| Low | | |

# Pre-Actions for the Incident

# Pre-Actions for the Incident

## Contact List

| Role | Name | Primary Location | Phone Number | Email |
|---|---|---|---|---|
| Someone | TL | 2F | 12345678 | incident@incident.com |
| Ops | Ops team | China | 1234556 | ops@incident.com |

# Pre-Actions for the Incident

## Rehearsal

- Take a recent incident to rehearsal with the whole team members

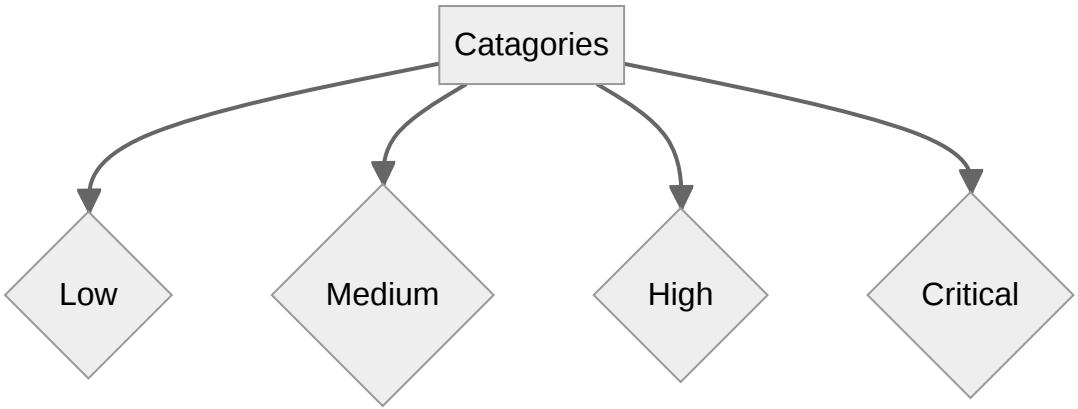
# Incident Response

# Incident Response

## YOU SHOULD

- Kep cool and calm
- Determine the severity
- Do NOT destroy any evidence

# Incident Response



# Incident Response

## Critical

- SIRT formed
- Requires executive level attention
- Emergency response
- Other requirements regarding incident response (e.g. from client side or compliance perspective) also should be taken into consideration.
- Requires senior leadership or MD review of incident report
- Triggers new Enterprise Risk Assessment and BCP review

# Post Actions of the Incident

# Post Actions of the Incident

## IR(Incident Report)

- docs

# Post Actions of the Incident

## Retro

- Go through the key point of the incident
  - Who… does what… when…
- Summary the executable actions for team
- Lesson and Learns

# Q&A

# Thank You!