

[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

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	<u>incident@incident.com</u>
Ops	Ops team	China	1234556	<u>ops@incident.com</u>

Pre-Actions for the Incident

Rehearsal

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

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

Q&A

Thank You!