PRO MANAGE

SOP FOR INCIDENT MANAGEMENT

Standard Operating Procedure for Incident Management

1.**Purpose**

This SOP outlines the steps to be taken in the event of an incident in the company, from reporting to resolution and follow-up. It aims to ensure a consistent and effective response to incidents, minimizing their impact and minimizing business disruption.

2. **Scope**

This SOP applies to all incidents that occur within the company, including security breaches, data loss, equipment failures, and other disruptions to normal operations.

3. **Incident Reporting**

- All incidents must be reported to the incident management team as soon as possible.
- The incident reporting process can be done through multiple channels such as email, phone, or a designated incident reporting portal.
- The report should include a detailed description of the incident, including the time it was discovered, location, and any relevant information about the incident.

4. **Incident Triage**

- Upon receipt of an incident report, the incident management team will assess the severity and impact of the incident and determine the appropriate response.
- The incident management team will categorize the incident based on its severity (high, medium, low) and assign a priority level (1, 2, 3, 4) based on the impact and urgency of the incident.
- The incident management team will activate the appropriate incident response plan based on the severity and priority level of the incident.

5. **Incident Response**

- The incident management team will initiate the incident response plan, which may involve activating the incident response team, isolating affected systems, and taking other necessary steps to contain the impact of the incident.

- The incident management team will continuously monitor the incident to ensure it is being effectively managed and resolved.
- The incident management team will provide regular updates to stakeholders and relevant parties on the status of the incident and any actions taken.

6. Investigation and Root Cause Analysis

- Once the incident has been contained, the incident management team will conduct an investigation to determine the root cause of the incident.
- The investigation will include a thorough review of logs, network traffic, and other relevant information.
- Based on the findings of the investigation, the incident management team will identify opportunities for improvement to prevent similar incidents from occurring in the future.

7. Communication

- The incident management team will develop a communication plan to keep stakeholders and relevant parties informed about the incident and the company's response.
- The communication plan will include regular updates on the status of the incident, including any actions taken and estimated resolution time.
- The communication plan will also include instructions for stakeholders and relevant parties on how to respond in the event of an incident.

8. Restoration

Once the incident has been resolved, the incident management team will work to restore normal operations and return to business as usual. The incident management team will perform a thorough review of the incident and the response to identify any areas for improvement.

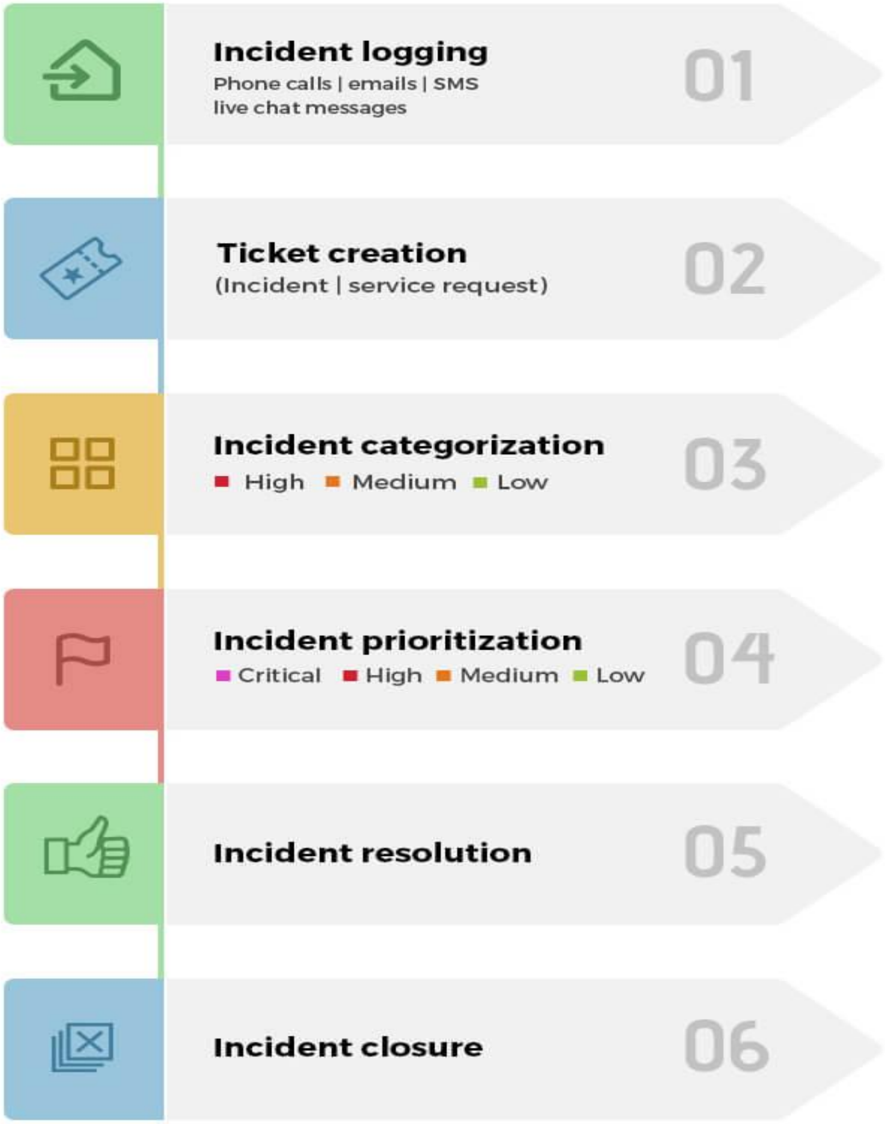
9. Post-incident Review

- The incident management team will conduct a post-incident review to evaluate the effectiveness of the incident response and identify opportunities for improvement.
- The post-incident review will include a review of the incident management process, communication plan, and incident response plan.
- The post-incident review will result in recommendations for changes to the incident management process, incident response plan, and communication plan to improve the company's ability to respond to future incidents.

10. **Conclusion**

The SOP for incident management is a critical component of the company's overall risk management strategy. It provides a consistent and effective approach to managing incidents, minimizing their impact.

WORKFLOW :


Incident logging
Phone calls | emails | SMS
live chat messages
01
Ticket creation
(Incident | service request)
02
Incident categorization
🟥 High 🟧 Medium 🟩 Low
03
Incident prioritization
🟪 Critical 🟥 High 🟧 Medium 🟩 Low
04
Incident resolution
05
Incident closure
06