Incident Management Plan

Introduction

Define the purpose of the incident management plan:

- How does this plan aim to protect [organization's name] and ensure continuous operations during and after an incident?

Define the scope of the incident management plan:

- What types of incidents does this plan cover?

Roles & Responsibilities

Responsibilities:

- What are the goals of each individual when dealing with an incident?

*See Contact Sheet for response team roles and contact information.

Identification

Define incident categories:

- What are the different incident categories and how are they defined in this plan?

Identify the severity of the incident:

- What criteria is used to determine the severity levels of an incident?

Incident Management Plan

Detection

Define the detection methods:

- What methods are being used to detect incidents? (Monitoring Tools, Alerting Tools, User Reports, Ticketing Software, etc.)

Define the reporting procedures:

- How should an incident be reported after detection?

*See incident reporting template.

Incident Response

Initial Assessment:

- What are the identified business impacts from the incident?

Immediate Action:

- What are the first steps that must be taken when an incident is detected?

Containment Strategy:

- What strategies will be used to contain this issue to prevent further damage?

Incident Management Plan

Incident Response (Continued…)

Eradication & Recovery:

- What strategies will be used to eradicate the root cause of this issue and restore the affected systems?

Communication Plan

Internal Communication:

- How and when will the response team communicate with internal stakeholders? (Alerting Tools, Mass Notifications, etc.)

External Communication:

- How and when will the response team communicate with external stakeholders? (Alerting Tools, Mass Notifications, etc.)

Incident Status Updates:

- How often will incident status updates be delivered, by what methods, and to who? (Alerting Tools, Mass Notifications, etc.)

Investigation & Analysis

Root Cause Analysis:

- What process will be use to determine the root cause of the incident?

Incident Management Plan

Investigation & Analysis (Continued…)

Documentation:

- How should incidents be documented during and after resolution?

Findings & Learnings:

- How will the findings from this incidents be documented and utilized for future incident management?

Post-Incident Review

Post-Incident Review Meeting:

- When and where will the post-incident review meeting be held for this incident?

Reporting:

- What information will be included in the post-incident report?

*See Post-Incident Review Template.

Improvement Plans:

- What insights can be use in the future and how will they be developed and implemented into the incident management plan?

*See Post-Incident Review Template.

Incident Management Plan

Conclusion

Summary & Key Findings:

- What are the key findings of this incident?

Approval

Incident Manager Name: _____

Incident Manager Signature: _____

Date: _____