FAIRDINKUM
LEVERAGING INNOVATION WITH TECHNOLOGY

Create Your Incident Response Plan

An incident response plan (IRP) for a company's technology infrastructure outlines procedures to detect, respond to and recover from technological or cybersecurity incidents. Preparing for such events is crucial to getting your business up and running again and reducing negative financial impact. These steps will help your business craft an IRP.

1 Introduction & Purpose

- **Overview:** Explain the purpose of the plan, including its objectives and scope.
- **Importance of Incident Response:** Highlight why the plan is critical for business continuity, data security, and compliance.

2 Roles & Responsibilities

- **Incident Response Team (IRT)**: Define the members of the IRT, their roles, and contact information.
- **Key Stakeholders:** Identify other departments or individuals who need to be informed or involved (e.g., legal, public relations, HR, IT).

3 Incident Categories & Classification

- **Types of Incidents:** List the types of incidents the company might face (e.g., malware, data breaches, weather/water damage, electrical outages, fires, etc.).
- **Severity Levels**: Provide guidelines on how to classify the severity of an incident (low, medium, high, critical).

4 Detection & Reporting

- **Incident Detection Mechanisms:** Describe the tools, systems, and processes used to detect incidents (e.g., intrusion detection systems, monitoring software, temperature monitors, security alerts and camera systems).
- **Reporting Procedures:** Define how to report an incident internally, including timelines and communication channels. May also contain how to report to any external services.

5 Communication Plan

- **Internal Communication:** Prepare guidelines for notifying internal stakeholders and departments during an incident.
- **External Communication:** Establish protocols for communicating with external parties (e.g., clients, partners, regulators, media).
- **Legal and Regulatory Requirements:** List mandatory reporting to regulatory bodies in case of data breaches or other legal obligations.

6 Documentation & Incident Tracking

- **Incident Log:** Outline procedures for documenting incidents, including a description, timeline, actions taken, and outcomes.
- **Root Cause Analysis (RCA):** Develop a process for conducting a root cause analysis to understand how and why the incident occurred.

7 Tools & Resources

- **Technology and Tools:** List tools used for detection, response, and recovery (e.g., firewalls, SIEM, forensic tools).
- **Third-Party Vendors:** Identify external resources or vendors involved in incident response (e.g., cybersecurity firms, legal counsel).

8 Escalation Procedures

- **When to Escalate:** Specify thresholds for escalating incidents to higher levels of management or external organizations.
- **Escalation Pathways:** Provide proper authority chain and steps for escalation within the company.

9 Training & Awareness

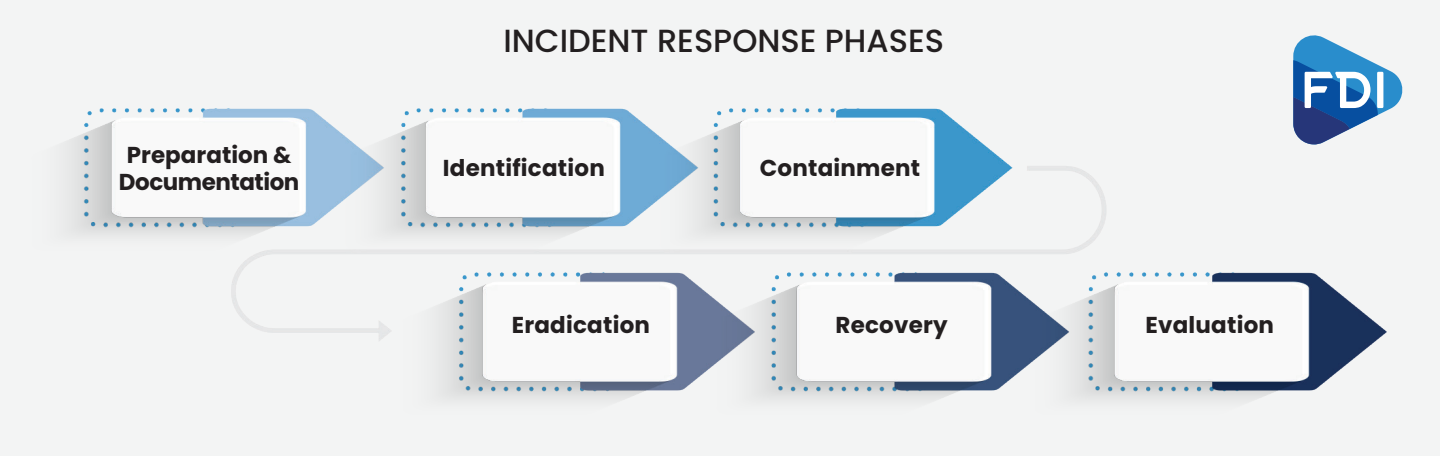
- **Employee Training:** Detail how employees are trained to recognize and report incidents.
- **IRT Drills and Simulations:** Conduct regular exercises to test the effectiveness of the incident response plan and team.

10 Review & Maintenance

- **Regular Updates:** Schedule periodic review and updates of the incident response plan. Should be reviewed at least annually.
- **Post-Incident Review:** Detail the process for reviewing incidents to ensure continuous improvement of the plan.
- **Legacy Services:** Note any legacy services or devices (if any) that are no longer applicable to an IRP to clearly lay out a reminder they are no longer involved.

11 Specifics & Appendices

- **Incident Response Checklist:** Detail step-by-step actions to be taken during different types of incidents. Very often these are one pager style documents of steps to go through on number 5 above. Incident Response Phase specifics for events can be handed out to anyone to be aware of what the previous and next courses of action are.
- **Contact Lists:** Update contact information for IRT members, vendors, and other relevant personnel.
- **Regulatory Requirements:** Specify legal obligations and compliance requirements based on the industry.



FAIRDINKUM
LEVERAGING INNOVATION WITH TECHNOLOGY
15 E 32nd Street, 9th Floor, New York, NY, 10016 • 212.624.3200 • fairdinkum.com