Incident Response Plan

An incident response plan outlines the steps taken to respond to and mitigate security incidents.

**Template Structure**:

1. **Title Page**
   * Document Title: "Incident Response Plan"
   * Author: Rick Abraham
   * Date
2. **Objective**
   * **Purpose**: Define the purpose of the incident response plan (e.g., to provide a clear, standardized response to security incidents).
   * **Scope**: Identify the types of incidents covered (e.g., malware, data breaches, unauthorized access).
3. **Roles and Responsibilities**
   * **Incident Response Team (IRT)**: Identify team members and their roles (e.g., Incident Commander, Communications Officer).
4. **Incident Identification and Classification**
   * Define how incidents are identified (e.g., monitoring tools, user reports).
   * Classify incidents by severity level (e.g., Low, Medium, High).
5. **Response Phases**
   * **Preparation**: Outline preventative measures and readiness checks.
   * **Detection and Analysis**: Describe how incidents are detected, logged, and analyzed.
   * **Containment, Eradication, and Recovery**: Steps to contain the threat, remove it, and restore normal operations.
   * **Post-Incident Review**: Analyze the incident to determine cause and prevention.
6. **Documentation Requirements**
   * Define what details to document during each phase (e.g., time of detection, actions taken).
7. **Testing and Review**
   * Outline plans for periodic testing of the incident response plan (e.g., quarterly or annually).