[Company Name] Incident Response Plan

**Document Version:** 1.0 **Date:** March 7, 2025

## 1. Overview

This Incident Response Plan (IRP) outlines the procedures [Company Name] will follow in the event of a security incident. It provides a structured approach to identifying, containing, eradicating, and recovering from security incidents, minimizing their impact on the business. This plan applies to all employees, contractors, and vendors.

## 2. Purpose

The purpose of this plan is to:

* Provide a clear and consistent response to security incidents.
* Minimize the damage and disruption caused by security incidents.
* Protect the confidentiality, integrity, and availability of company data and systems.
* Ensure compliance with relevant regulations and legal requirements.
* Facilitate a timely and effective recovery from security incidents.
* Learn from incidents to improve security posture.

## 3. Scope

This plan covers all security incidents that could potentially impact [Company Name]’s information systems, data, or operations. This includes, but is not limited to:

* **Malware Infections:** Viruses, worms, trojans, ransomware.
* **Unauthorized Access:** Hacking attempts, unauthorized logins, data breaches.
* **Denial of Service (DoS) Attacks:** Attacks that disrupt access to company systems or networks.
* **Data Loss or Theft:** Loss or theft of company data, devices, or physical documents.
* **System Failures:** Hardware or software failures that compromise security.
* **Physical Security Breaches:** Unauthorized access to company facilities.
* **Social Engineering Attacks:** Phishing, baiting, pretexting.

## 4. Policy

### 4.1. Incident Response Team (IRT)

* An Incident Response Team (IRT) is established to manage and coordinate the response to security incidents.
* The IRT will consist of the following members:
  + **Team Leader:** [Owner/CEO/Designated Person] - Overall responsibility for the incident response process.
  + **Technical Lead:** [IT Support (Internal or External)] - Responsible for technical aspects of incident handling (containment, eradication, recovery).
  + **Communications Lead:** [Office Manager/Designated Person] - Responsible for internal and external communications related to the incident.
* The IRT may be augmented with additional personnel as needed, depending on the nature and severity of the incident.

### 4.2. Incident Response Phases

The incident response process will follow these phases:

1. **Preparation:**
   * Develop and maintain this Incident Response Plan.
   * Establish and train the Incident Response Team.
   * Implement security controls to prevent incidents.
   * Conduct regular risk assessments and vulnerability scans.
   * Maintain up-to-date contact information for the IRT and key personnel.
   * Back up critical data regularly.
2. **Identification:**
   * Monitor systems and networks for signs of suspicious activity.
   * Detect and report potential security incidents.
   * All employees are responsible for reporting suspected security incidents to the IRT immediately.
   * The IRT will assess reported incidents to determine if they are actual security incidents.
3. **Containment:**
   * Isolate affected systems or networks to prevent further damage or spread.
   * Implement short-term fixes to limit the impact of the incident.
   * Preserve evidence for further investigation.
4. **Eradication:**
   * Remove the root cause of the incident (e.g., malware removal, vulnerability patching).
   * Verify that the threat has been completely eliminated.
5. **Recovery:**
   * Restore affected systems and data from backups.
   * Verify that systems are functioning normally.
   * Implement long-term fixes to prevent recurrence.
6. **Post-Incident Activity (Lessons Learned):**
   * Conduct a post-incident review to analyze the incident and the response.
   * Identify areas for improvement in the Incident Response Plan and security controls.
   * Document lessons learned and implement changes to prevent similar incidents in the future.
   * Update the incident response plan as needed.

### 4.3. Incident Reporting

* All suspected security incidents must be reported immediately to [Designated Contact - e.g., IT Support, Office Manager, Owner].
* The report should include as much detail as possible, such as:
  + Date and time of the incident.
  + Description of the incident.
  + Systems or data affected.
  + Any observed symptoms or error messages.
  + Contact information of the reporter.

### 4.4. Communication

* The Communications Lead will be responsible for communicating with internal and external stakeholders, as needed.
* Communication will be timely, accurate, and appropriate for the audience.
* Legal counsel may be consulted before releasing information to external parties.

### 4.5. Evidence Handling

* All evidence related to the incident (e.g., logs, system images, malware samples) must be preserved carefully.
* Chain of custody procedures will be followed to ensure the integrity of evidence.

## 5. Compliance

Failure to comply with this plan may result in disciplinary action.

## 6. Revision History

| Version | Date | Author | Description of Change |
| --- | --- | --- | --- |
| 1.0 | March 7, 2025 | Shijie Yin | Initial Plan Creation |