**Incident Response Plan Template**

**1. Introduction** This Incident Response Plan (IRP) outlines the procedures and responsibilities for identifying, responding to, and recovering from cybersecurity incidents at [Your Organization Name]. The goal is to minimize impact, recover operations, and improve future responses.

**2. Objectives** - Detect and respond to incidents swiftly - Minimize impact on operations - Recover affected systems and data - Communicate effectively with stakeholders - Document and analyze incidents

**3. Scope** This IRP applies to all information systems, networks, personnel, and third parties involved in handling or processing [Your Organization Name]’s data.

**4. Roles and Responsibilities** - **Incident Response Team (IRT):** Lead and coordinate all response activities. - **IT Staff:** Provide technical support, implement containment and recovery. - **Communications Lead:** Handle internal and external communications. - **Legal and Compliance:** Ensure regulatory compliance and legal considerations.

**5. Incident Classification** Incidents are classified by severity: - **Low:** No impact on operations (e.g., phishing attempt blocked) - **Medium:** Limited impact (e.g., minor system disruption) - **High:** Significant impact (e.g., data breach, ransomware)

**6. Incident Response Phases** 1. **Preparation:** - Conduct training and simulations - Maintain updated contact lists and tools 2. **Identification:** - Detect and report suspected incidents - Assess and classify the incident 3. **Containment:** - Short-term: Limit immediate damage (e.g., isolate affected systems) - Long-term: Implement fixes to prevent recurrence 4. **Eradication:** - Remove threats and vulnerabilities from the environment 5. **Recovery:** - Restore affected systems and verify functionality 6. **Lessons Learned:** - Conduct post-incident review - Update policies and improve controls

**7. Communication Plan** - Notify affected parties and stakeholders promptly - Provide regular updates during major incidents - Follow legal and regulatory notification requirements

**8. Documentation and Reporting** - Maintain logs of all activities and decisions - Produce an incident report after each event

**9. Training and Testing** - Conduct regular training sessions for the IRT - Perform annual IRP tests and simulations

**10. Plan Review and Updates** - Review the IRP at least annually or after significant incidents - Update contact information and responsibilities as needed

**11. Contact Information** - **Incident Response Team Lead:** [Name, Phone, Email] - **IT Security Contact:** [Name, Phone, Email] - **Legal/Compliance Contact:** [Name, Phone, Email]

**12. Approval and Revision History** - Approved by: [Name/Title] - Effective Date: [Date] - Next Review Date: [Date]