Blue Light IT
Cyber Resilience Experts

Incident Response Plan

Incident Response Plan

Here's a simple, Incident Response Plan (IRP) template for small CPA firms.
If you need help customizing it, contact us to discuss info@bluelightit.com.

Disclaimer

This Incident Response Plan (IRP) template is provided by Blue Light IT (BLIT) as a general guide to help small CPA firms develop a response framework for security incidents. It is intended for informational purposes only and does not constitute legal, regulatory, or cybersecurity advice.

Every business has unique requirements, risks, and operational contexts. This template should be customized to align with your firm's specific needs, technology, and compliance obligations. Blue Light IT (BLIT) assumes no responsibility for the accuracy, completeness, or applicability of this template to your business.

For professional advice or assistance in developing a tailored incident response plan, consult a qualified cybersecurity or legal professional.

Want to learn more?

Let's talk – book a meeting

Incident Response Plan (IRP)

For: [Your Firm Name]
Effective Date: [Insert Date]

1. Purpose

This Incident Response Plan (IRP) outlines procedures for identifying, responding to, and recovering from security incidents that impact the confidentiality, integrity, or availability of client data.

2. Incident Response Team (IRT)

- **Incident Coordinator:** [Name, Title, Contact Information]
- **Backup Coordinator:** [Name, Title, Contact Information]
- **Key Contacts:**
  - IT Support: [Name, Contact Info]
  - Legal Advisor: [Name, Contact Info]
  - External Cybersecurity Partner: [Name, Contact Info]

3. Incident Response Phases

A. Preparation

- Train employees to recognize and report incidents (e.g., phishing, malware).
- Maintain contact lists for internal and external resources.
- Ensure backups and disaster recovery plans are in place.

B. Identification

- Determine whether an event qualifies as a security incident by asking:
  - Does it involve unauthorized access, disclosure, or use of client data?
  - Has any system been disrupted or compromised?
- Document incident details, including:
  - Date/Time of discovery
  - Person reporting the incident
  - Systems or data affected

C. Containment

- **Short-Term Actions:**
  - Disconnect affected devices from the network.
  - Disable compromised accounts.
- **Long-Term Actions:**
  - Apply patches, update credentials, and strengthen security controls.

D. Eradication

- Remove malware, unauthorized accounts, or other vulnerabilities.
- Confirm the threat has been fully neutralized.

E. Recovery

- Restore affected systems from backups.
- Monitor systems for abnormal activity post-incident.
- Resume normal business operations once verified as safe.

F. Lessons Learned

- Conduct a post-incident review to:
  - Determine root causes.
  - Identify areas for improvement.
  - Update the Incident Response Plan as needed.

4. Reporting Incidents

- Notify affected clients and stakeholders if their data is involved.
- Report to regulatory authorities as required by law.
- Provide incident details, corrective actions, and mitigation steps.

5. Documentation

Maintain a record of all incidents, including:

- Description of the incident
- Actions taken during each phase
- Outcomes and lessons learned

6. Testing and Review

- Test the IRP annually or after major updates.
- Update the plan to address changes in technology, regulations, or operations.

Approval and Acknowledgment

This IRP has been approved by [Owner/Manager Name]. All employees must read and acknowledge their roles in incident response.

Approved By:
[Name, Title, Signature]
[Date]