1(888)-575-7973
info@lighthouseintegrations.com

Incident Response Plan (IRP) Template

A Framework for Businesses of Any Size or Industry

Introduction

How to Use This Template

This Incident Response Plan (IRP) template is designed to give your organization a clear structure for managing unexpected events that could disrupt your operations. It is built to be industry-agnostic, meaning whether you're in healthcare, finance, manufacturing, retail, or professional services, the structure applies.

You'll notice each section includes fillable fields, checklists, and tables. These are prompts. Simply replace the blank lines with information that applies to your business. The examples included (like "Incident Lead" or "Low/Medium/High/Critical" severity levels) are starting points. You should adapt, remove, or expand them to reflect how your business actually works.

This plan will help you:

- Clarify roles and responsibilities during a crisis.
- Establish consistent communication channels internally and externally.
- Document and learn from past incidents to improve future resilience.
- Meet regulatory or industry compliance requirements (if applicable).

Remember: this document is not a substitute for legal or compliance advice. If your industry has strict reporting or security regulations, consult with professionals to ensure your plan meets those obligations.

I started Lighthouse because I believe businesses of every size deserve to feel secure, confident, and ready for the future. An Incident Response Plan is about protecting your people, your reputation, and your ability to keep moving forward when challenges arise. This template is our gift to you. Use it, make it your own, and take a step toward a stronger, more resilient future.

Kevin Bobroske
President & Founder
Lighthouse Integrations

Table of Contents

Plan Overview

This section gives a high-level summary of the Incident Response Plan (IRP). It identifies ownership, version control, and review cycles so that the document stays current and reliable.

Field	Details
Document Owner:	
Version Number:	
Date Created:	
Last Update:	
Next Review Date:	
Approved By:	

Purpose & Scope

The purpose of the IRP is to establish a structured approach to identifying, managing, and resolving incidents that may impact business operations, information security, or customer trust. Having this written down ensures that everyone understands the "why" behind the plan and uses it consistently when needed.

Purpose Statement

Describe in one or two sentences the goal of this IRP. For example:

"The purpose of this Incident Response Plan is to minimize business disruption, protect sensitive data, and ensure rapid recovery from incidents."

Scope

When defining the scope of your Incident Response Plan, think about where incidents can happen, who they affect, and what needs protection. This ensures your plan isn't too vague to be useful, but also not so narrow that big gaps are left uncovered.

Here are areas you should consider when defining scope:

- **Core IT Systems** – *servers, networks, business apps, cloud services, mobile devices.*
- **Customer-Facing Platforms** – *websites, e-commerce, apps, or client portals.*
- **People** – *employees, contractors, vendors, and anyone with system or data access.*
- **Physical Locations** – *offices, data centers, and remote/home work setups.*
- **Data** – *customer info, financial records, employee files, intellectual property.*
- **Vendors & Third Parties** – *external providers who manage or process your data.*
- **Exclusions (Optional)** – *routine IT issues (like password resets) that don't need full incident escalation.*

Roles & Responsibilities

This section defines the Incident Response Team (IRT) and clarifies who is responsible for decision-making, technical actions, communications, and oversight during an incident. Assigning roles in advance avoids duplication, delays, and miscommunication.

Recommended Roles

Role	Responsbilities	Primary Contact	Backup Contact	Contact Information
Incident Lead	Oversees the incident response process, coordinates team actions, escalates decisions to leadership.			
Technical Lead	Analyzes root cause, contains and eradicates the threat, restores systems.			
Communication Lead	Manages internal and external messaging; ensures updates are accurate and timely.			
Legal/Compliance Contact	Advises on legal obligations, regulatory reporting, contracts, and data privacy concerns.			
Executive/Senior Management Contact	Makes high-level business decisions; authorizes resources, budget, or downtime.			
HR Contact	Manages employee-related incidents (insider threats, policy violations, social engineering targeting staff).			

Incident Classification

Not all incidents are created equal. Some are minor annoyances, while others can shut down operations or trigger legal reporting requirements. Classifying incidents into severity levels helps the team prioritize response, allocate resources, and escalate appropriately.

Low
Minor disruption with no sensitive data at risk. Usually handled by IT/helpdesk.

Medium
Noticeable disruption or limited data exposure. May affect a small group of users or systems.

High
Major disruption, significant data loss, or potential regulatory involvement. Immediate team response required.

Critical
Severe impact on business operations, financial stability, or customer trust. Requires executive involvement and possibly public disclosure.

Examples of Incidents

- Low – *Accidental deletion of a non-critical file, minor service outage.*
- Medium – *Phishing attempt reported by several employees, temporary system outage impacting one department.*
- High – *Malware infection spreading across multiple systems, data breach involving sensitive but limited information.*
- Critical – *Ransomware attack shutting down core systems, confirmed theft of large volumes of customer data, major compliance breach.*

Incident Response Lifecycle

The Incident Response Lifecycle is a repeatable framework for handling any type of incident, whether it's a cyberattack, system outage, or physical disruption. By following these six phases, you ensure your responses are organized, consistent, and effective. Skipping steps or improvising often leads to confusion, longer downtime, and missed learning opportunities.

1. Preperation

Preparation ensures your team, tools, and policies are in place before something happens. It's much easier to follow a plan that already exists than to create one in the middle of a crisis.

Examples:

- Train employees to recognize and report incidents (e.g., phishing attempts, suspicious logins).
- Keep security tools (antivirus, firewalls, monitoring) updated and functional.
- Maintain accurate documentation: system inventories, escalation paths, contact lists.
- Ensure backups are recent and tested.

Our preperation activities include...

2. Identification

This is the process of detecting and confirming whether an event is truly an incident. Many events are false alarms so this step prevents wasted time.

Examples:

- Define how incidents are reported (helpdesk, hotline, ticket system, email).
- Document when, where, and how the incident was discovered.
- Classify the incident's severity (see Incident Classification Section).
- Verify legitimacy: Is this a malicious activity, a system misconfiguration, or a user error?

Our identification process looks like...

3. Containment

Stopping the damage from spreading while keeping essential operations running. Think of this as putting a bandage on the wound before deeper treatment.

Examples:

- Short-term containment: immediately isolate affected systems, accounts, or networks.
- Long-term containment: apply patches, implement network segmentation, or migrate services to a secure environment.
- Balance speed vs. stability: shutting down too much can harm operations, while doing too little can let the attack spread.

Our containment strategies are...

4. Eradication

Removing the root cause of the incident so it cannot reoccur. This goes beyond containment, its also about cleaning up and fixing what caused the problem.

Examples:

- Remove malware, malicious accounts, or unauthorized devices.
- Patch vulnerabilities that were exploited.
- Reset compromised passwords or disable accounts.
- Validate that no hidden backdoors remain.

Our eradication steps include...

5. Recovery

How you will safely restore systems and return back to normal operations. This phase balances urgency with caution because rushing can lead to reinfection or recurring problems.

Examples:

- Restore systems from clean backups.
- Validate that systems are stable and functioning correctly.
- Monitor closely for unusual behavior in the days/weeks following recovery.
- Communicate clearly with affected stakeholders once stability is confirmed.

Our recovery procedure includes...

6. Lessons Learned

A structured review of what happened, how well the team responded, and how to improve. It transforms each incident into a learning opportunity. This step is one of the most valuable to your business going forward.

Examples:

- Hold a debrief meeting within 1–2 weeks of the incident.
- Document the incident timeline, actions taken, and outcomes.
- Identify gaps: Did detection take too long? Was communication unclear?
- Update the IRP, policies, and training based on insights.

From each incident, we will record lessons learned such as...

Communication Plan

Clear communication prevents confusion and panic during an incident. It ensures the right people are informed at the right time, avoids misinformation, and keeps employees, customers, and regulators confident in your organization's ability to respond.

Communication Categories

Internal Notifications

Best practices for notifying your internal team:

- Notify relevant teams immediately (IT, management, security).
- Share only verified facts.
- Use pre-approved channels (secure chat, phone tree, or internal alerts).

External Notifications

Best practices for notifying vendors and partners:

- Notify external parties only after initial containment (to avoid spreading panic).
- Provide clear, concise instructions if action is required (e.g., password reset).
- Ensure messaging is consistent with internal updates.

Regulatory Notifications

Best practices for notifying regulators and authorities:

- Know your legal obligations in advance.
- Document what was reported, when, and to whom.
- Assign this responsibility to a Legal/Compliance role to avoid mistakes.

Public Statements (If Required)

Best practices for communicating to the press, social media, or customers:

- Prepare draft templates for common scenarios (e.g., service outage, data breach).
- Keep it simple, honest, and factual — avoid technical jargon.
- All public statements should be cleared by Communications Lead + Executive contact.

Audience	Responsible Party	Method	Timeline
Internal Teams	Incident Lead	Secure Chat/ Phone Call	Immediately
Executives	Incident/ Technical Lead	Email/Phone	Within 1 Hour
Customers	Communications Lead	Email/ Website Notice	If Affected
Vendors/ Partners	Communications Lead	Email/Phone	As Needed
Regulators (If Required)	Legal/ Compliance Contact	Formal Notice	As Required By Law
Public/Media	Communications Lead & Executive	Press Release/ Social Media	If Incident is Critical

Tips for Success

- Keep contact lists updated. A communication plan is useless if the phone numbers are outdated.
- Decide in advance who approves external messages. Nothing slows response more than waiting for sign-off.
- Document every notification. This protects you legally and provides a record for post-incident reviews.

Tools & Resources

This section lists the systems, applications, and resources your organization will rely on during incident response. Having this documented ensures that when time is critical, the team doesn't waste energy figuring out what tools are available or how to access them.

Detection & Monitoring Tools

These help you spot incidents as early as possible:

- Antivirus/endpoint protection software
- SIEM (Security Information and Event Management) systems
- Log monitoring tools
- Intrusion detection/prevention systems (IDS/IPS)

Our monitoring tools include:

Communication Channels

Reliable communication is key during a crisis. Examples:

- Secure messaging apps (Slack, Teams, Signal)
- Emergency phone tree / call list
- Incident ticketing or tracking system

Our communication methods are:

Response & Recovery Tools

The hands-on tools that let you stop, fix, and restore. Examples:

- Backup and recovery systems
- Patching tools
- Remote access tools
- Forensic analysis software (if available)

Our response tools include:

Documentation & Tracking Resources

Where you'll store evidence, notes, and logs during and after the incident.
Examples:

- Incident log template (see Section 8)
- Ticketing system (Jira, ServiceNow, etc.)
- Secure document storage (SharePoint, Notion, Google Drive)

Our documentation resources are:

Communication Channels

Reliable communication is key during a crisis. Examples:

- Secure messaging apps (Slack, Teams, Signal)
- Emergency phone tree / call list
- Incident ticketing or tracking system

Our communication methods are:

Response & Recovery Tools

The hands-on tools that let you stop, fix, and restore. Examples:

- Backup and recovery systems
- Patching tools
- Remote access tools
- Forensic analysis software (if available)

Our response tools include:

Appendix

The appendix is your space to customize this plan further. While the core template covers universal best practices, every organization has unique requirements. Use this section to capture additional details that apply to your business, industry, or region.

Industry-Specific Notes

Depending on your industry, you may need to document specific requirements or reporting obligations here. Some examples:

- Healthcare (HIPAA): Note how you will report patient data breaches and protect personal health information.
- Finance (PCI-DSS, SOX): Document processes for protecting payment card data, reporting fraud, or meeting audit requirements.
- Manufacturing/OT: Include procedures for securing industrial control systems or addressing safety concerns.
- Small Business: You might simply record a streamlined escalation process, noting which roles may be combined due to team size.

References & Resources

This is a list of standards, frameworks, or guidance your business may align with.

- NIST Computer Security Incident Handling Guide (SP 800-61 Rev. 2)
- ISO/IEC 27035: Information Security Incident Management
- CISA (Cybersecurity & Infrastructure Security Agency) Guidance
- Local/Regional Regulations: GDPR (EU), HIPAA (US healthcare), PIPEDA (Canada), or others relevant to your operations.

Looking for more guidance when it comes to building your Incident Response Plan? Book a free consultation: Schedule Your Consultation Here