FILL-IN TEMPLATE

Incident Response Plan Template

A lightweight, editable starting point for your organization's incident response plan. Replace the bracketed fields, add or remove steps to match your environment, and review it with leadership at least annually.

How to use this template: Fill in every field marked [bracketed text]. An example entry is shown in italics under each section as a guide. Delete the examples once you've filled in your own information.

1. Purpose & Scope

This plan defines how **[Company Name]** detects, responds to, and recovers from cybersecurity incidents affecting **[systems/data in scope, e.g., "all corporate networks, cloud environments, and customer data"]**.

Example: This plan defines how Acme Manufacturing detects, responds to, and recovers from cybersecurity incidents affecting all corporate networks, cloud environments, and customer/employee data.

2. Roles & Responsibilities

Role	Name / Title	Responsibility	Contact
Incident Commander	[Name/Title]	Owns the response, makes final decisions	[Phone/Email]
IT/Security Lead	[Name/Title]	Leads technical investigation & containment	[Phone/Email]
Legal Counsel	[Name/Title or Firm]	Advises on notification & liability	[Phone/Email]
Communications Lead	[Name/Title]	Manages internal/external messaging	[Phone/Email]
Executive Sponsor	[Name/Title]	Authorizes major decisions (e.g., ransom, disclosure)	[Phone/Email]
Cyber Insurance Carrier	[Carrier Name]	Claims & breach coach coordination	[Policy # / Hotline]

3. Incident Classification

Severity	Definition	Response Target
Critical	[e.g., active ransomware, confirmed data exfiltration, system-wide outage]	[e.g., immediate — 24/7 response]
High	[e.g., confirmed unauthorized access, isolated malware infection]	[e.g., within 2 hours]
Medium	[e.g., suspicious activity requiring investigation]	[e.g., within 1 business day]
Low	[e.g., policy violation, low-risk phishing report]	[e.g., within 3 business days]

© 2026 Cenova Cyber, LLC

4. Response Steps by Phase

- ☐ **Detect** [How incidents are identified — monitoring alerts, employee report, vendor notification, etc.]
- ☐ **Contain** [Immediate steps to stop the spread — isolate systems, disable accounts, block IPs]
- ☐ **Eradicate** [Steps to remove the threat — patch, rebuild, remove malicious access]
- ☐ **Recover** [Steps to restore normal operations — restore from backup, validate integrity]
- ☐ **Notify** [Who must be notified and within what timeframe — regulators, customers, insurer, law enforcement]
- ☐ **Review** [Post-incident review process — what happened, what worked, what changes are needed]

5. Communication Plan

Internal notification order: [e.g., Incident Commander → Executive Team → All Staff]

External notification triggers: [Define what triggers customer, regulator, or public notification]

Breach notification deadline: [e.g., within 60 days per HIPAA, or per applicable state/federal law]

6. Key Contacts

Contact	Name/Org	Phone	Notes
Cyber Insurance / Breach Coach	[Name]	[Phone]	[Policy #]
Outside Counsel	[Firm]	[Phone]	
Managed Security Provider	Cenova Cyber	[Phone]	cenovacyber.com
Law Enforcement (FBI/IC3)	Local Field Office	[Phone]	ic3.gov

Review cadence: *This plan should be reviewed and tested via tabletop exercise at least annually, and updated after any real incident or major infrastructure change.*

Need Help Building This Out?
Cenova Cyber can help you customize and test a complete incident response plan.
Contact us to get started.
www.cenovacyber.com