**Delete This Page Before Creating Your Company’s Template**

**About This Document**

This Incident Response Plan (IRP) outlines how to prepare for, respond to, and recover from cybersecurity incidents. It defines the people, processes, and tools your organization should activate when a cyber threat emerges—minimizing downtime, protecting your data, and ensuring legal/regulatory compliance.

1. **How to Use This Plan**
2. **Prepare**: Assign your response team, define roles, and update contact info.
3. **Respond**: Follow the incident lifecycle from detection to recovery.
4. **Refine**: Use post-incident reviews to improve and update the plan regularly.
5. This document is designed for easy adaptation to your environment. Combine it with the **Incident Progress Report (IPR)** template to ensure proper documentation and response tracking during real-world incidents.

**About SpecGravity**

At SpecGravity, we specialize in simplifying technology operations for multiunit brands in hospitality, retail, and fast-scaling environments. Our cybersecurity services are built for agility and real-time protection, helping you navigate the complexities of today's threat landscape.

How We Help

* Immediate Incident Response:  
  Rapid containment, forensic investigation, and communication support when every minute counts.
* Prevention & Readiness:  
  We provide proactive solutions such as 24/7 monitoring, endpoint protection, vulnerability management, and employee training.
* Ongoing Support:  
  Through managed cybersecurity services, compliance guidance, and scalable solutions, we help you stay resilient and compliant long-term.

Need Help During or After an Incident?  
Reach out to our cybersecurity team at:  
📧 info@specgravity.com  
📞 1-844-700-4728  
🌐 [www.specgravity.com](http://www.specgravity.com)

**[Company Name] Cybersecurity Incident Response Plan (IRP)**

**Prepared By**: Full Name

**Preparer Contact Info**: Email / Phone

**1. Purpose**

This Incident Response Plan (IRP) outlines the policies, roles, and procedures for detecting, responding to, managing, and recovering from cybersecurity incidents. The goal is to minimize impact, restore operations swiftly, and comply with legal, regulatory, and contractual obligations.

**2. Scope**

This plan applies to all employees, systems, applications, and data managed or supported by [Company Name]. It covers internal systems, customer-facing platforms, third-party integrations, and physical access security breaches with a cyber component.

**3. Incident Response Team (IRT)**

| **Role** | **Name** | **Contact** | **Responsibilities** |
| --- | --- | --- | --- |
| **Incident Commander** |  |  | Overall coordination, decision-making |
| **Security Analyst** |  |  | Investigation, containment, and root cause |
| **IT Lead** |  |  | Infrastructure remediation and recovery |
| **Legal/Compliance** |  |  | Regulatory and legal communication |
| **Communications Lead** |  |  | Stakeholder and public relations communication |

**4. Incident Categories & Severity Levels**

| **Category** | **Examples** |
| --- | --- |
| **Phishing** | Suspicious emails, credential harvesting |
| **Malware** | Ransomware, spyware, viruses |
| **Unauthorized Access** | Stolen credentials, privilege misuse |
| **Data Breach** | PII, PHI, financial info exfiltration |
| **Denial of Service** | DDoS attacks disrupting service availability |

**Severity Levels**

* **High – Major data loss, critical system outage, legal impact**
* **Medium – Contained access, no confirmed data loss**
* **Low – Suspicious activity with no immediate impact**

**5. Incident Lifecycle & Procedures**

**5.1 Identification**

* Log detection method (SIEM alert, employee report, etc.)
* Triage alert severity
* Assign incident ticket and notify the IRT

**5.2 Containment**

* Isolate affected systems (network segmentation, user lockdown)
* Take forensic images (before wiping/rebooting)
* Prevent further spread

**5.3 Eradication**

* Remove malicious files/accounts
* Patch vulnerabilities
* Reset credentials and access points

**5.4 Recovery**

* Restore from clean backups
* Validate system integrity
* Monitor for signs of reinfection

**5.5 Lessons Learned**

* Conduct post-incident review (within 7 days)
* Update IRP and training plans
* Document findings in the IPR (Incident Progress Report)

**6. Communication Plan**

* Internal Notifications: All affected departments, leadership
* External Notifications: Legal counsel, regulators, clients, media
* Template Messaging: Use pre-approved statements to avoid misinformation

**7. Evidence Handling & Chain of Custody**

* Log all artifacts (logs, disk images, emails)
* Maintain chain of custody documentation
* Secure storage for forensic review and possible litigation

**8. Compliance Requirements**

**Include relevant laws/regulations such as:**

* GDPR
* CCPA
* HIPAA
* PCI-DSS
* SOX
* Industry-specific requirements

**9. Testing & Training**

* Tabletop Exercises: Run biannually with IRT
* Employee Awareness: Annual training on incident reporting
* Drills: Simulate phishing and malware response quarterly

**10. Document Control**

* Plan Owner: Name / Role
* Last Reviewed: YYYY-MM-DD
* Next Review Due: YYYY-MM-DD
* Version: v1.0