Incident Response Plan

Step-by-step playbook for security incident management

This template provides a structured incident response plan covering preparation, identification, containment, eradication, recovery, and lessons learned. It includes severity classification, escalation procedures, and communication templates.

Prepared by: Nuvencia — Information Security Advisory

Author: Jaouhar Mosbahi, CISSP, CCSP, ISO 27001 LI/LA

Version: 1.0 — February 2026

Classification: Template — Customise for your organisation

This template is provided by Nuvencia for guidance purposes. Organisations should customise it to reflect their specific context, risk appetite, and regulatory requirements.

© 2026 Nuvencia. All rights reserved.

1. Preparation

Establish the incident response capability before incidents occur:

- Define and train the Incident Response Team (IRT) with clear roles
- Establish and communicate the incident reporting channel (e.g., security@[domain], hotline)
- Maintain an up-to-date asset inventory and network diagrams
- Ensure logging and monitoring tools are operational
- Conduct regular tabletop exercises (at least annually)
- Maintain relationships with external parties (legal counsel, forensics provider, regulators)

1.1 Incident Response Team

Role	Responsibility	Contact
Incident Commander	Overall coordination and decision-making	[Name / Phone]
Technical Lead	Technical investigation and containment	[Name / Phone]
Communications Lead	Internal and external communications	[Name / Phone]
Legal Advisor	Legal and regulatory guidance	[Name / Phone]
Executive Sponsor	Strategic decisions and resource allocation	[Name / Phone]

2. Severity Classification

Severity	Description	Response Time	Escalation
Critical (P1)	Active data breach, ransomware, system-wide compromise	Immediate	CEO, Legal, Regulator
High (P2)	Confirmed intrusion, significant data exposure risk	< 1 hour	CISO, Senior Mgmt
Medium (P3)	Malware detection, phishing compromise, policy violation	< 4 hours	CISO, IT Lead
Low (P4)	Suspicious activity, failed attacks, vulnerability discovery	< 24 hours	Security Team

3. Identification

- Monitor alerts from SIEM, EDR, and security tools
- Validate the alert — confirm whether it is a true positive
- Classify the incident type (malware, phishing, data breach, DoS, insider threat)
- Assign severity level using the classification above
- Document initial findings in the incident log

4. Containment

- Short-term: Isolate affected systems to prevent spread

© 2026 Nuvencia. All rights reserved.

- Disable compromised accounts and revoke sessions
- Block malicious IPs, domains, or file hashes at the perimeter
- Preserve evidence — take forensic images before remediation
- Long-term: Apply temporary fixes while preparing for eradication

5. Eradication

- Remove malware, backdoors, and attacker persistence mechanisms
- Patch exploited vulnerabilities
- Reset credentials for all affected accounts
- Review and harden configurations
- Verify eradication is complete before moving to recovery

6. Recovery

- Restore systems from verified clean backups
- Gradually bring systems back online with enhanced monitoring
- Verify system integrity and normal operation
- Monitor for signs of re-compromise for 30-90 days
- Communicate recovery status to stakeholders

7. Lessons Learned

- Conduct a post-incident review within 5 business days
- Document timeline, root cause, impact, and response effectiveness
- Identify improvement actions and assign owners
- Update playbooks, procedures, and detection rules
- Share sanitised learnings with the broader team

© 2026 Nuvencia. All rights reserved.