ACME Corporation: Incident Response Policy

Type of Policy: Administrative

Effective Date: November 2025

Last Revised: November 2025

Review Date: January 2026

Policy Owner: ACME Corporation Chief Information Security Officer

Contact Name: John Kasket

Contact Title: Chief Information Security Officer

Contact Email: johnkasket@acmecorp.com

Purpose

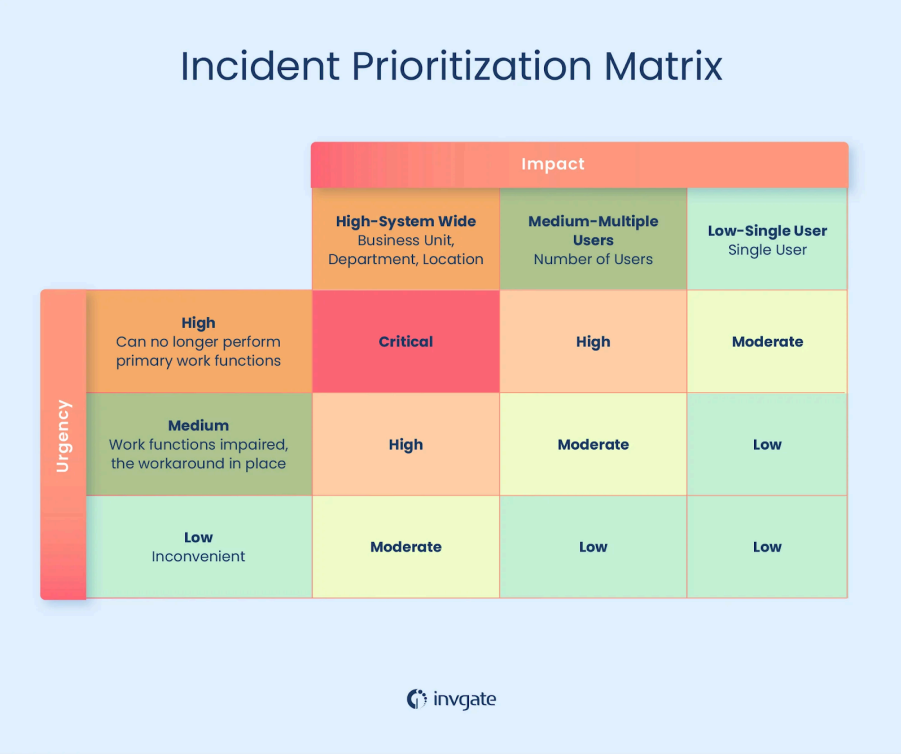
The ACME Corporation Incident Response Policy defines how ACME Corporation identifies, reports, investigates, and recovers from cybersecurity incidents and system disruptions with a structured incident approach following Cyber Security Incident Response Team (CSIRT) standards. This 2025 policy will replace the previous Cyber Security Policy (March 2020).

Scope

The ACME Corporation Incident Response Policy applies to all ACME Corporation employees, contractors, vendors, third-party service providers, and any individual with access to ACME IT resources. The policy applies to both on-site and remote access.

Incident Classification

Incidents are categorized into four severity levels using the Incident Prioritization Matrix:



- **Critical:** Ransomware attacks, confirmed breach of restricted data, or major service outages. These types of incidents demand escalation to CISO.
- **High:** Unauthorized access to confidential systems or widespread malware. These must be escalated within an hour.
- **Medium:** Isolated malware or repeated suspicious login activities.
- **Low:** Policy violations without confirmed compromise or low-risk alerts do not require urgent escalation.

Incident Response Phases

1. **Preparation**
    a. All ACME employees are properly trained through the annual security awareness training regarding their incident response roles and responsibilities.
2. **Identification**
    a. Identifying whether or not the system has been breached by discovering when it happened, who discovered it, how it was discovered, and what is the scope of the impact.
3. **Containment**
    a. With the goal of containing the spread to not cause further damage, employees must disconnect affected devices from the internet, patch the systems, and change user access credentials and passwords depending on the scope of the breach.
4. **Eradication**
    a. Eliminate the root cause of the breach by removing all malware, hardening and patching systems, and applying any updates. These actions could be through a third-party vendor, if needed.
5. **Recovery**
    a. Restore and return affected systems and devices to production.
6. **Lessons Learned**
    a. Analyze and document everything about the breach to create an updated response plan.

Incident Response Triage Function

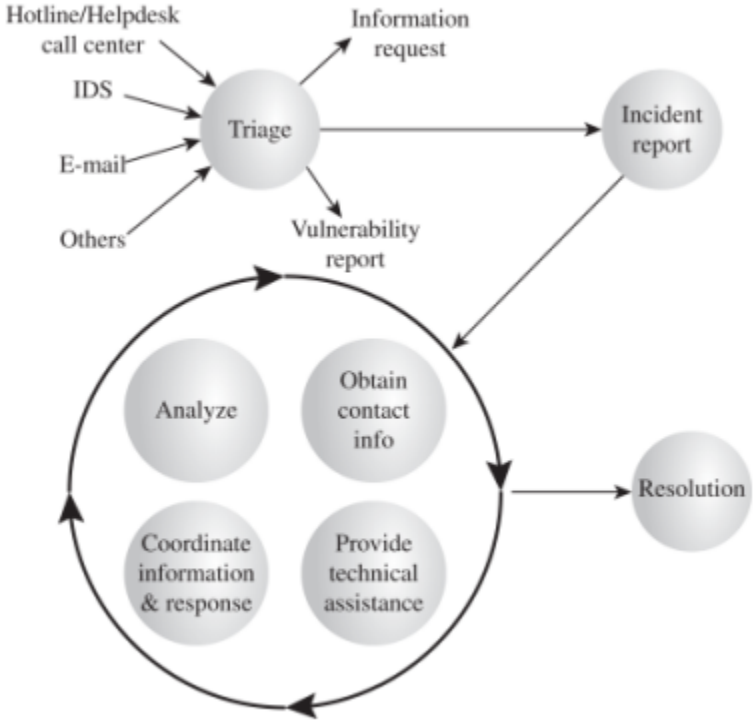


Figure 17.2 Incident Handling Life Cycle

Evidence Handling

Logs, screenshots, system images, and user reports may be used as evidence if deemed essential for documenting incidents or supporting ongoing investigative needs. Employees must not alter system data or attempt to investigate incidents independently. All evidence must be preserved for security teams to analyze using company-approved tools and methods.

Chief Information Security Officer

The Chief Information Security Officer is responsible for creating and maintaining a cybersecurity program and leading the ACME Corporation Cyber Security Team. The purpose of the cybersecurity program is to maintain the confidentiality, integrity, and availability of

corporate IT Resources and data. In addition, the Chief Information Security Officer, or a designee, is responsible for leading the investigation of and response to cybersecurity incidents.

Enforcement

Violations of this policy may result in the loss of ACME Corporation system and network usage privileges, and/or disciplinary action, up to and including termination, as outlined in applicable ACME Corporation policies. To report suspected instances of ethical violations, please visit ACME Corporation's Ethics Hotline, a secure and confidential reporting system.

Policy Review

This policy shall be reviewed annually and updated as necessary to address emerging threats, technological changes, and regulatory requirements.

References

Danby, S. (2024, November 13). *ITIL Priority Matrix: How to use it for incident, problem, service request, and Change Management*. The Service Desk and IT Service Management blog. https://blog.invgate.com/itil-priority-matrix

Stallings, W., & Brown, L. (2024). *Computer security: Principles and practice* (5th ed.). Pearson.

Ellis, D. (n.d.). *6 Phases in an Incident Response Plan*. Securitymetrics.com. https://www.securitymetrics.com/blog/6-phases-incident-response-plan