ACME Corporation: Vulnerability and Patch Management 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 Vulnerability and Patch Management Policy establishes a comprehensive approach to identifying and assessing security vulnerabilities in ACME systems with proper use of patching and remediation to minimize risks and preserve system integrity.

Scope

The ACME Corporation Vulnerability and Patch Management 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.

Asset Inventory

The ACME Corporation must maintain an updated inventory of hardware devices, installed software, operating systems, and cloud resources. Each asset must have an assigned owner or be documented in storage locations. The assigned owner is responsible for verifying device accuracy and ensuring frequent updates. Inventories must be reviewed quarterly with consistent document modifications.

Vulnerability Scanning

The ACME Security Team is responsible for consistent vulnerability scanning on all devices and software to find potential vulnerabilities, as well as compare them to a vulnerability database. The database records common vulnerabilities and exposures (CVEs) for the various hardware and software. The identified risks must be reviewed by staff and assigned to appropriate employees or third-party vendors for immediate remediation.

Patch Management Requirements

- All patches must ensure rigorous testing to prevent disruption of system integrity
- Emergency patches may be applied immediately during active threats.
- Unsupported software must be updated, removed, and documented.
- Administrators must verify successful installation and patching results.

All patch deployment schedules must align with vulnerability severity and operational needs.

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

Kosinski, M., & Forrest, A. (2025, September 16). *What is vulnerability scanning?*. IBM. https://www.ibm.com/think/topics/vulnerability-scanning