ACME Corporation: Cybersecurity 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 Cybersecurity Policy (CSP) establishes a comprehensive information security program to provide the guiding principles for protecting the confidentiality, integrity, and availability of corporate data and IT resources. This 2025 policy will replace the previous Cyber Security Policy (March 2020).

Scope

The ACME Corporation Cybersecurity Policy (CSP) 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.

Security Governance

With security governance as the foundation of ACME's cybersecurity strategy, the Chief Information Security Officer (CISO) is responsible for working with department leaders to consider emerging risks through protective measure implementations. All ACME personnel share responsibility for protecting company information. Employees must practice secure data handling, identify suspicious activities, and comply with relevant company policies.

Risk Management

Through annual risk assessments or whenever new critical systems are introduced, these assessments help ACME identify vulnerabilities that must be categorized, prioritized, and assigned for remediation or acceptance. Following established guidelines in the Identity &

Access Management Policy, these new systems are required to have appropriate safeguards in place to ensure secure storage of sensitive or restricted data.

Security Architecture

ACME's security architecture is built on principles such as Zero Trust and Least Privileged. These principles guide the configuration of ACME's networks, systems, and cloud environments. As outlined in the Identity and Access Management Policy, all users are:

- Required to have verification of devices and users before granting access to IT resources
- Implementing layers of security such as firewalls, endpoint protection, and secure authentication
- Documenting any baselines for servers, workstations, cloud environments, and personal devices.

Cloud and Network Security

Cloud-based security must follow ACME's security standards through configurations that restrict unauthorized access, enforce encryption, and provide visible logs for ACME's monitoring system. Network security must implement firewalls and continuous traffic monitoring, along with limiting any unauthorized devices without express approval from IT security**.**

Identity & Access Management

Multi-factor authentication, password standards, account provisioning, and privileged access, as outlined in the Identity and Access Management Policy, are required.

Security Monitoring and Incident Response

All activity must be collected and reviewed regularly in the system logs. Any unauthorized access attempts or malicious activity must be escalated to the security team according to the severity. All monitoring activities must comply with the Data Privacy and Acceptable Use Policy. All employees must report security incidents following procedures defined in Policy 4: Incident Response.

Vulnerability and Patch Management

All requirements for scanning, prioritizing vulnerabilities, and deploying security patches are defined in the Vulnerability and Patch Management Policy.

Data Protection and Privacy

All requirements for the collection, use, storage, and distribution of data are governed by the Vulnerability and Patch Management Policy.

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

Stallings, W., & Brown, L. (2024). *Computer security: Principles and practice*. Pearson Education Limited.