ACME Corporation: Data Privacy & Acceptable Use 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 Data Privacy and Acceptable Use Policy defines how ACME Corporation collects, stores, uses, and protects personal and business data. This policy outlines user expectations, privacy protections, data requirements, and proper use of company resources. This 2025 policy will replace the previous Data Privacy Policy (March 2020).

Scope

The ACME Corporation Data Privacy and Acceptable Use 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.

Data Classification Levels

1. **Public Data**
   a. Information intended for external disclosure, such as job postings or marketing materials.
2. **Internal Data**
   a. Information restricted to ACME employees and approved third-party vendors. Examples include policies and project documentation. Internal data requires basic safeguards to restrict access and secure collaboration tools.
3. **Confidential Data**
   a. Sensitive business or customer information, such as internal financial documents or customer order histories. Access to confidential data must be limited to authorized personnel based on business need.

4. **Restricted Data**
    a. The highest sensitivity level with sensitive information such as financial account numbers, health information, and user credentials. This type of data requires encryption, MFA, and consistent monitoring. Any employees handling restricted data must adhere to Policy 2: Identity and Access Management.

Data Requirements

ACME collects only the minimum amount of personal data required for legitimate business purposes, including but not limited to customer information needed to provide services and employee information for work management. Access to restricted data must only be given to authorized individuals with the required business need, with unauthorized viewing, copying, or sharing of any kind strictly prohibited.

Acceptable Use

ACME's IT resources, such as computers, internet access, software applications, and communications systems, must be used only for business purposes. Personal use is not permitted as it violates policy and consumes unnecessary system resources.

Prohibited activities include:

- Accessing illegal, inappropriate, or harmful content
- Installing unauthorized software
- Attempting to bypass security controls
- Using ACME systems for personal business ventures or fraudulent activity
- Sharing passwords or storing restricted data on unapproved personal devices.

Monitoring and Privacy Expectations

Any use of ACME systems implies consent to monitoring as ACME's IT and Security team regularly reviews logs, network traffic, and device activity to ensure compliance with corporate policies. ACME does not monitor personal content on personal devices beyond what is necessary for security if those devices access company systems.

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

Vigo, J. (2024, August 5). Acceptable use policies for employees. Workplace Technology. Acceptable Use Policies for employees. Workplace technology. https://www.jamf.com/blog/acceptable-use-policy-for-workplace-technology/

Data Classification (Data Management): A complete overview. Spirion. (2024, October 3). https://www.spirion.com/data-classification#:~:text=Data%20classification%20categories,PHI%2C%20and%20credit%20card%20information.