# ACME Corporation: Identity and Access 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 Identity and Access Management (IAM) Policy outlines the procedures for verifying users, granting access, and securing authentication across all ACME systems. IAM constructs user safeguards to prevent unauthorized access, privilege mishandling, and credential compromise. This 2025 policy will replace the previous Password Policy (March 2020).

**Scope**

The ACME Corporation Identity and Access Management Policy (ISP) 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.

**Identity Management**

Identity management ensures that user accounts are created, updated, and removed securely. The onboarding process must include identity verification, assignment of appropriate role-based access following the Least Privileged Principle, and mandatory security training. Accounts must be modified when users change responsibilities. Upon employee termination, account removal must occur immediately, as former employees or contractors must not have access to ACME systems under any circumstances.

**Access Control Principles**

Access controls must be implemented based on:

- Role-Based Access Control (RBAC): A security framework that restricts system access based on the authorized user's role in their organization.

- Least Privilege: A security concept that limits users to only the minimum level of access required to perform their specific tasks.
- Need-to-Know: A security principle that limits access to classified/sensitive information to only those personnel who require it for their job responsibilities.

**Authentication Requirements**

Multi-factor authentication (MFA) is required for remote access, administrative actions, email accounts, and any handling of sensitive data. Passwords must follow ACME's set Password Standards. Any default credentials must be updated upon employment.

**Password Standards**

Standard user passwords must be at least 16 characters long with a random mix of upper/lowercase letters, numbers, and symbols, or a passphrase of 5-7 unrelated words.
All default, "out of the box" usernames and passwords are required to be changed before any implementation of the systems.

**Account Provisioning Procedures**

1. The requester submits an access request through the IT service team with a clear indication of their role and related systems.
2. Manager either approves or denies the request after confirming the business need.
3. IT provisions account according to RBAC and notifies the requester through email.
4. Any new users must complete the required security awareness training before activation.

**Account Deprovisioning Procedures**

HR notifies IT immediately upon employee termination. IT disables accounts immediately upon notice, based on priority, and completes full deprovisioning within 24 hours. Contractor and temporary accounts include an automatic expiration date.

**Account Modification**

1. A role change request gets sent to the IT service team.
2. IT service team reviews the existing permissions and denies or approves after confirming the business need.
3. Notifies the user through email.

**Password Reset and Recovery Procedures**

Users may reset their passwords by completing MFA verification.

**Monitoring and Logging**

- Authentication events, privilege escalations, failed login attempts, and account lockouts must be logged.
- Security teams must be alerted upon suspicious activity such as multiple geographic logins or repeated failed attempts.
- Logs supporting security investigations must be kept for a minimum of 1 year unless other retention rules apply.

**Auditing**

- Quarterly audits must verify that all provisioning, deprovisioning, modification, and access review procedures are followed accordingly.
- Any findings must be remediated and alerted to the CISO.

**Security Awareness Training**

All users must complete security awareness training annually or during onboarding.

**Incident Response Integration**

IAM-related incidents must be escalated to the Security Response Time according to Policy 4: Incident Response.

**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**

*Glossary*. CSRC. (n.d.). https://csrc.nist.gov/glossary

Fleischmann, E. (2022, July 25). *Need to know principle*. Implementing the Need-To-Know principle ▸ Redlings. https://www.redlings.com/en/guide/need-to-know

America's Cyber Defense Agency. (n.d.). *Require strong passwords | CISA*. CISA. https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-strong-passwords