ACME Inc. Password Policy

1. Purpose

The purpose of this Password Policy is to ensure that all ACME Inc. systems, applications, and data are protected through strong authentication mechanisms that prevent unauthorized access. This policy establishes requirements for password creation, management, storage, and protection in accordance with **ISO/IEC 27001:2022 (Annex A.5.17, A.8.2, A.8.4)** and **SOC 2 Security and Confidentiality principles**.

---

2. Scope

This policy applies to:

- All ACME Inc. employees, contractors, consultants, vendors, and third parties who access company systems.
- All systems and applications (on-premises, cloud, SaaS) that authenticate using passwords or passphrases.
- Administrative, user, service, and system accounts.

---

3. Policy Objectives

- Ensure strong password protection for all information assets.
- Minimize the risk of unauthorized system access.
- Establish consistent password standards across the organization.
- Comply with ISO 27001 and SOC 2 control requirements.

---

4. Roles and Responsibilities

Role	Responsibility

IT Security Team	Enforce, monitor, and periodically review password configurations.
System Administrators	Configure systems in compliance with this policy.
Employees/Users	Create and manage passwords as per defined standards.
Compliance Team	Verify adherence during internal audits and compliance reviews.

---

5. Password Requirements

5.1. Password Complexity

All user and administrative account passwords must meet the following requirements:

Requirement	Description
Minimum Length	12 characters for standard users, 14+ for privileged accounts
Character Mix	Must include uppercase, lowercase, number, and special character
Passphrase Option	Allowed if minimum length is ≥ 16 characters (e.g., “BlueSky_Runs@Morning2025”)
No Personal Info	Must not include personal data (name, username, DOB, etc.)
No Common/Leaked Passwords	Must be checked against a database of breached passwords (e.g., HaveIBeenPwned or local password filter)

5.2. Password Expiration

Account Type	Expiration
Standard User Accounts	Every 180 days
Privileged/Admin Accounts	Every 90 days
Service/System Accounts	Annually (review and rotation required)

5.3. Password Reuse

- Users cannot reuse any of their **last 5 passwords**.
- Passwords must differ by at least **4 characters** from previous passwords.

5.4. Account Lockout

To mitigate brute force attempts:

- **Lockout after:** 5 failed attempts
- **Lockout duration:** 15 minutes (or manual reset by admin)
- **Incremental delay:** Enforced after 3 failed attempts

5.5. Storage and Transmission

- Passwords must be **hashed and salted** using approved algorithms (e.g., bcrypt, Argon2, PBKDF2).
- Passwords must **never be stored or transmitted in plaintext**.
- For integrations, **OAuth2, SAML, or secure token-based authentication** must be preferred over static passwords.

---

6. Multifactor Authentication (MFA)

- MFA is **mandatory** for:
  - All privileged and administrative accounts
  - Remote access (VPN, RDP, cloud portals, etc.)
  - Access to sensitive systems (finance, HR, customer data)
- MFA methods: hardware token, authenticator app, biometric, or smart card.

7. Service and API Accounts

- Must use **strong, randomly generated** passwords (minimum 24 characters).
- Passwords must be **stored securely** in a **vault** (e.g., HashiCorp Vault, AWS Secrets Manager).
- Shared credentials are **strictly prohibited**.
- Access and usage logs must be **monitored and reviewed** quarterly.

8. Password Sharing and Disclosure

- Passwords **must not be shared** via email, chat, or written on physical media.
- Shared access (e.g., team accounts) must use group-based authentication mechanisms or password vaults.
- Any suspected password compromise must be **reported immediately** to IT Security.

9. Temporary Passwords

- Must be **unique, random**, and **expire after first use**.
- Temporary credentials should only be issued through **secure channels** (e.g., internal helpdesk portal).

10. Password Reset Procedures

- Identity verification must be conducted before resetting a password.
- Self-service password reset tools must require MFA.

- All password reset requests must be **logged** for audit purposes.

---

11. Audit and Review

- Password configurations must be **reviewed quarterly**.
- Compliance audits (internal or external) will verify adherence to ISO 27001 Annex A.8.2 and SOC 2 CC6.1, CC6.3 controls.
- Exceptions must be documented, risk-assessed, and approved by the CISO.

---

12. Enforcement

Non-compliance with this policy may result in:

- Temporary suspension of access privileges.
- Disciplinary actions as per HR and IT Security guidelines.
- Review and remediation of systems found non-compliant.

---

13. References

- ISO/IEC 27001:2022 — Annex A.5.17 (Authentication Information Management), A.8.2 (Identity Management), A.8.4 (Access Control).
- SOC 2 Security and Confidentiality Trust Services Criteria — CC6.1, CC6.2, CC6.3.
- NIST SP 800-63B: Digital Identity Guidelines.
- OWASP Authentication Cheat Sheet.

---

14. Revision and Approval

Version	Date	Description	Approved By
1.0	14 Oct 2025	Initial version aligned with ISO 27001:2022 and SOC 2	CISO – ACME Inc.