ACME CORPORATION – INFORMATION SECURITY POLICY

Version: 1.0
Effective date: 01/01/2025
Owner: Chief Information Security Officer (CISO)

1. Purpose

The purpose of this Information Security Policy is to define the principles, responsibilities, and controls required to protect ACME Corporation's information assets against unauthorized access, disclosure, alteration, and destruction.

This policy supports regulatory and contractual obligations, including but not limited to ISO 27001, data protection laws, and customer security requirements.

2. Scope

This policy applies to:

- All employees, contractors, and third parties who access ACME systems or data.
- All information assets, including on-premise systems, cloud environments, laptops, mobile devices, and SaaS applications.
- All stages of the information lifecycle: creation, processing, storage, transmission, archiving, and disposal.

3. Roles and Responsibilities

3.1 CISO

- Owns and maintains this policy.
- Approves security standards and procedures.
- Coordinates incident response activities.

3.2 IT Security Team

- Implements technical security controls (firewalls, access control, logging, monitoring).
- Performs vulnerability assessments and follows up on remediation.
- Supports investigations of security incidents.

3.3 Department Managers

- Ensure that users in their area follow this policy.

- Approve access rights to applications and shared resources under their responsibility.
- Report suspected security incidents immediately.

3.4 All Users

- Must protect credentials and devices.
- Must not share passwords or MFA tokens.
- Must immediately report any suspected loss, theft, or misuse of information or systems.

4. Access Control

4.1 General Principles

- Access to information and systems shall be granted on a **need-to-know** and **least privilege** basis.
- Access rights must be tied to job roles and reviewed regularly.

4.2 User Provisioning and De-provisioning

- New user accounts shall only be created based on a documented request approved by a manager.
- Changes to user roles, transfers, and terminations shall be reflected in system access rights within 24 hours.
- Accounts of leaving employees must be disabled on or before their last working day.

4.3 Authentication

- All users shall authenticate with a unique user ID and a strong password or MFA, where available.
- Passwords must be at least 12 characters and not reused across personal and corporate services.
- Shared generic accounts (like “admin”, “guest”) must be avoided. Where technical constraints require them, their use shall be strictly controlled and logged.

4.4 Access Reviews

- System owners must review user access rights for critical systems at least once every six months.
- Excessive, unused, or inappropriate access must be removed promptly.
- Access review results must be documented and kept for audit purposes.

5. Asset Management

5.1 Asset Inventory

- All information assets (servers, applications, databases, laptops, mobile devices) must be recorded in an asset inventory.
- Each asset must have a designated owner responsible for classification and protection.

5.2 Information Classification

- Information shall be classified at least into the following categories: Public, Internal, Confidential, and Restricted.
- Owners must assign a classification level and ensure appropriate handling rules are defined.

6. Cryptography and Encryption

6.1 Data in Transit

- Confidential and Restricted information transmitted over untrusted networks (e.g., the internet) shall be encrypted using strong protocols such as TLS 1.2 or higher.
- Unencrypted transmission of credentials or sensitive data via email or instant messaging is prohibited unless additional protection (e.g., encrypted attachments, secure file transfer) is used.

6.2 Data at Rest

- Confidential and Restricted information stored on laptops and mobile devices shall be protected with full-disk encryption.
- Server-side encryption shall be enabled for databases and storage volumes containing sensitive information, where supported.

6.3 Key Management

- Encryption keys shall be generated, stored, rotated, and revoked according to documented key management procedures.
- Access to encryption keys shall be limited to authorized personnel only.

7. Logging and Monitoring

7.1 Logging Requirements

- Security-relevant events such as login attempts, privilege changes, configuration changes, and access to sensitive data shall be logged on critical systems.

- Logs shall include at least: user ID, timestamp, source IP (where available), and action performed.

7.2 Log Protection and Retention

- Logs shall be protected against tampering and unauthorized access.
- Security logs for critical systems must be retained for at least 12 months, or longer where regulatory requirements apply.

7.3 Monitoring

- The IT Security Team shall regularly review logs and alerts from security tools (e.g., SIEM, IDS/IPS, EDR).
- Suspicious activities must be investigated and escalated according to the Incident Management process.

8. Incident Management

8.1 Definition
A security incident is any event that has resulted in, or has a significant likelihood of resulting in, unauthorized access, disclosure, modification, or destruction of information or disruption of services.

8.2 Reporting

- All users are required to report suspected or confirmed security incidents immediately to the Service Desk or Security Team.
- Reports can be made by phone, email, or ticketing system, according to local procedures.

8.3 Incident Response Process
The following steps shall be followed for all security incidents:

1. Detection and Reporting – identify and report the incident.
2. Triage and Classification – assess severity, impacted systems, and data.
3. Containment – limit the scope and impact (e.g., disable accounts, isolate systems).
4. Eradication – remove the root cause, such as malware or misconfigurations.
5. Recovery – restore services and verify that systems are clean.
6. Lessons Learned – document the incident, root cause, and corrective actions.

8.4 Communication

- External communication about incidents (e.g., to regulators, customers, media) shall be handled by authorized roles only, such as Legal, CISO, or Communications.

- Users must not share incident details on social media or with unauthorized parties.

9. Backup and Recovery

9.1 Backup Requirements

- Critical systems and data must be backed up regularly according to business requirements.
- Backup frequency shall be defined per system (e.g., daily incremental, weekly full backup).

9.2 Backup Protection

- Backups containing Confidential or Restricted information must be encrypted and stored securely.
- Access to backups shall be restricted and monitored.

9.3 Testing

- Restoration tests must be performed at least annually to verify that backups can be successfully restored within required timeframes.

10. Third-Party and Supplier Management

10.1 Security Requirements for Suppliers

- Third-party suppliers that process ACME's Confidential or Restricted information must sign appropriate data protection and confidentiality agreements.
- Where applicable, suppliers shall be required to implement controls aligned with ISO 27001 or equivalent standards.

10.2 Due Diligence and Monitoring

- Prior to onboarding, critical suppliers shall undergo security due diligence.
- Security requirements and responsibilities shall be documented in contracts or service agreements.
- Significant changes affecting the supplier's security posture shall be reviewed and addressed.

11. Acceptable Use

- Users shall not install unauthorized software on corporate devices.
- Use of peer-to-peer file sharing or unapproved cloud storage for corporate data is prohibited.

- Personal use of corporate resources must not interfere with work responsibilities or violate laws and regulations.

12. Training and Awareness

- All employees must complete information security awareness training at least annually.
- Additional role-based training shall be provided to administrators, developers, and other sensitive roles.
- Completion of training shall be tracked and reported to management.

13. Policy Exceptions

Exceptions to this policy shall be formally documented, including:

- Business justification
- Risk assessment
- Compensating controls
- Approval by the CISO (or delegate)
- Validity period of the exception

14. Enforcement

Violation of this policy may result in disciplinary action up to and including termination of employment, contract termination, and legal action, where applicable.

15. Review and Maintenance

This policy shall be reviewed at least annually or whenever significant changes occur to the organization, technology, or regulatory environment.

Policy Owner: CISO
Next Review Date: 01/01/2026