ACME Corporation Cybersecurity Policy Set

Policy 1: Information Security Policy

Purpose

The purpose of the Information Security Policy is to establish a comprehensive security framework that protects the confidentiality, integrity, and availability of ACME Corporation's information assets. This policy outlines the roles, responsibilities, and expectations for preserving the security of data and systems throughout the organization. It also serves as the foundational document for ACME's cybersecurity program, providing guidance for security governance, risk management, system architecture, cloud security, and monitoring practices. ACME's overall security posture is reinforced through collaboration among technical teams, security leadership, and all end users.

Scope

This policy applies to all employees, contractors, interns, and third-party personnel who use ACME systems, networks, or data. It applies to all ACME-owned or ACME-managed hardware, software, cloud services, data repositories, and digital assets. These requirements also extend to remote work environments and off-site access to ACME systems.

Security Governance

Effective governance is a foundational component of ACME's cybersecurity strategy. The Chief Information Security Officer (CISO) is responsible for designing, implementing, and maintaining the Information Security Program. The CISO works with department leaders to evaluate emerging risks, implement protective measures, and monitor the effectiveness of security controls. Managers are accountable for ensuring that their teams follow security procedures, complete mandatory training, and promptly report incidents.

All ACME personnel share responsibility for protecting company information. Employees must practice secure handling of data, identify suspicious activity, and comply with all relevant policies. Team members must also participate in regular training opportunities and remain aware of phishing attempts, social engineering tactics, and evolving security threats.

Risk Management

ACME conducts risk assessments annually and whenever new critical systems are introduced. Risk assessments help identify system vulnerabilities, data sensitivity levels, and potential business impacts. Once risks are identified, they must be categorized, prioritized, and assigned for remediation, mitigation, or acceptance.

Business units must work with security teams to implement appropriate security controls. Systems that store or process sensitive or restricted data require additional safeguards based on data classification guidelines established in Policy 3. Any system changes, upgrades, or new integrations must undergo a security review to evaluate potential risks prior to deployment.

Security Architecture

ACME's security architecture is built on principles such as Zero Trust, Defense in Depth, Least Privilege, and Secure-by-Design. These principles guide the configuration of networks, systems, and cloud environments. All user access must follow strict identity and access standards as outlined in **Policy 2: Identity and Access Management**.

Security architecture includes the following requirements:

- Verification of users and devices before granting access to resources.
- Implementation of layered controls such as firewalls, endpoint protection, monitoring tools, and secure authentication.
- Documentation and enforcement of configuration baselines for servers, workstations, cloud environments, and mobile devices.

Cloud and Network Security

Cloud-based resources must use approved providers and comply with ACME's security configuration standards. Cloud services must be configured to restrict unauthorized access, enforce encryption, and provide logging visibility to ACME's monitoring systems.

Network controls include segmentation of production, testing, and guest networks; use of firewalls; and continuous traffic monitoring. Unauthorized devices may not connect to the network without approval from IT security. Network access must remain limited, regularly reviewed, and monitored for anomalies.

Endpoint Security

Endpoints such as laptops, desktops, and mobile devices must be protected by company-approved antivirus tools, automatic updates, and host-based firewalls. Full-disk encryption is required for devices containing ACME data, and lost or stolen devices must be reported immediately. Mobile devices must be enrolled in mobile device management (MDM) to ensure secure configuration and remote wipe capability.

Identity & Access Management (Cross-Reference)

All access control requirements—including multi-factor authentication (MFA), password standards, account provisioning, and privileged access—are defined in **Policy 2: Identity and Access Management**. This policy defers to Policy 2 for all identity-related controls.

Security Monitoring and Incident Response

System logs must be collected and reviewed regularly to detect unauthorized access attempts or malicious activity. Alerts must be escalated to the security team according to severity. Monitoring activities must comply with privacy expectations outlined in Policy 3.

Employees must report security incidents immediately, and all incident responses follow the procedures defined in **Policy 4: Incident Response and Business Continuity**.

Vulnerability and Patch Management (Cross-Reference)

All requirements for scanning, prioritizing vulnerabilities, and deploying security patches are governed by **Policy 5: Vulnerability and Patch Management**.

Data Protection and Privacy

All security controls involving the collection, use, storage, and distribution of data must align with **Policy 3: Data Privacy and Acceptable Use**. ACME employees must handle confidential and restricted data appropriately and avoid sharing sensitive information through unapproved channels.

Enforcement

Failure to comply with this policy may lead to disciplinary measures, including written warnings, suspension of access rights, or termination. Severe negligence or intentional policy violations may result in legal action.

Policy 2: Identity and Access Management

Purpose

The Identity and Access Management (IAM) Policy defines how ACME verifies identities, grants access, and secures authentication across all systems. IAM ensures that users are granted appropriate access based on their roles and responsibilities. It also establishes safeguards to prevent unauthorized account use, privilege misuse, and credential compromise.

Scope

This policy applies to all ACME users—including employees, contractors, interns, and third parties—who access ACME systems, applications, or data. The policy applies to both on-site and remote access.

Identity Lifecycle Management

Identity lifecycle management ensures that user accounts are created, updated, and removed consistently and securely. The onboarding process must include identity verification, assignment of appropriate role-based access, and enrollment in mandatory security training.

Accounts must be modified when users change roles or responsibilities. Account removal must occur immediately upon employee separation. Former employees or contractors may not retain access to ACME systems under any circumstances.

Access Control Principles

Access controls must be implemented based on:

- **Least Privilege:** Users receive minimum access necessary.
- **Need-to-Know:** Access to sensitive data requires business justification.
- **Separation of Duties:** Administrators and employees who handle sensitive processes must not have conflicting responsibilities.
- **Role-Based Access Control (RBAC):** Users follow standard role templates, reducing the need for manual permissions.

Authentication Requirements

Authentication methods must validate user identity effectively. MFA is required for remote access, administrative actions, email accounts, and systems handling sensitive data. Passwords must follow ACME's complexity standards, including length requirements and prohibitions on common or compromised passwords.

Default credentials must be updated before a system moves into production. Biometric authentication may supplement but not replace other factors.

Password Standards

Standard user passwords must be at least 12 characters long. Privileged accounts require a minimum of 16 characters or passphrases with multiple words. Passwords may not be reused or shared, and password managers must be used to securely store credentials.

Privileged Access Management

Privileged users such as system administrators must use dedicated administrative accounts that are monitored separately. Their actions must be logged and subject to review. Temporary privilege elevation may be granted for limited tasks with automatic expiration.

Access Reviews

Managers must review user access rights quarterly to ensure they reflect current job duties. Privileged account reviews must occur monthly. Access inconsistent with user roles must be removed immediately.

Provisioning and Deprovisioning Procedures

Account Provisioning

1. Requestor submits access request through the IT service portal and indicates required role or systems.

2. Manager approves request and confirms business need.

3. IT provisions account according to predefined RBAC templates and notifies the requestor.

4. New users must complete required security awareness training within 5 business days of account activation.

Account Modification

- Role changes trigger a review of existing permissions; IT adjusts access within 1 business day of approved request.

Account Deprovisioning

- HR notifies IT immediately upon employee separation. IT disables accounts within 4 hours of notification and completes full deprovisioning within 24 hours. Contractor and temporary accounts include an automatic expiration date.

Password Reset and Recovery Procedures

Self-Service Reset

- Users may use the self-service portal to reset passwords after completing MFA verification.

- Temporary passwords issued by helpdesk must be changed on first login.

Help Desk Assisted Reset

- Help desk staff must verify identity using multiple verification steps (manager confirmation, government ID, or pre-registered recovery methods) before issuing temporary credentials.

- All assisted resets are logged for audit purposes.

Privileged Access Request Process

1. Submit a privileged access request via PAM/IT portal with justification and time-bound duration.

2. Manager approval required; security review for high-risk systems.

3. PAM issues time-limited credentials or enables just-in-time elevation.

4. Privileged sessions are recorded and retained according to retention schedules.

Single Sign-On (SSO) and Federation

ACME deploys SSO for supported applications to centralize authentication and simplify logging. Identity federation with approved third-party services is permitted when contracts and security reviews are completed and MFA is enforced.

Third-Party and Vendor Access

Third-party accounts must be unique and issued only for the duration of the engagement. Vendor access must use least-privilege principles and be logged. Vendors must authenticate using corporate-approved mechanisms and comply with ACME security requirements defined in vendor contracts.

Monitoring and Logging

- Authentication events, privilege escalations, failed login attempts, and account lockouts must be logged centrally.
- Security teams must alert on anomalous authentication patterns such as impossible travel, multiple geographic logins, or repeated failed attempts.
- Logs supporting security investigations must be retained for a minimum of 1 year unless other retention rules apply.

Auditing and Compliance

- Quarterly audits verify that provisioning, deprovisioning, and access review procedures are followed.
- Findings from audits must be remediated on a timeline commensurate with risk and reported to the Security Steering Committee.
- Compliance with IAM standards is part of performance reviews for system owners and relevant administrators.

Training and Awareness

- All users must complete IAM-related training (password hygiene, MFA use, phishing recognition) during onboarding and annually thereafter.
- Administrators receive role-specific IAM training focused on privileged access controls, logging, and secure administration practices.

Exceptions and Risk Acceptance

- Exceptions to IAM controls require documented justification and approval from the CISO.
- Temporary exceptions include expiration dates and compensating controls and must be reviewed at least quarterly.

Incident Response Integration

- IAM-related incidents (compromised credentials, suspicious privilege use) must be escalated to the Security Team and handled according to **Policy 4: Incident Response and Business Continuity**.

- Rapid deprovisioning and forced credential rotation are primary containment actions for suspected compromise.

Enforcement and Consequences

- Violations of IAM policy (e.g., password sharing, willful misuse of privileges) may result in disciplinary actions up to termination.

- Repeated negligence in complying with access reviews or privileged account management may result in revocation of administrative privileges and performance consequences.

Definitions (Selected)

- **MFA (Multi-Factor Authentication):** Use of two or more factors (something you know, something you have, something you are) to verify identity.

- **RBAC (Role-Based Access Control):** A method of restricting system access to authorized users based on role definitions.

- **PAM (Privileged Access Management):** Tools and processes that control and monitor use of privileged accounts.

Integration With Other Policies

IAM connects directly with the following policies:

- Data classification requirements: **Policy 3**

- Incident response procedures: **Policy 4**

- Vulnerability response for identity-related exposures: **Policy 5**

Policy 3: Data Privacy and Acceptable Use Policy

Purpose

The purpose of the Data Privacy and Acceptable Use Policy is to define how ACME Corporation collects, stores, uses, and protects personal and business data. This policy outlines user behavior expectations, privacy protections, data classification requirements, and the proper use of company technology resources. By establishing clear rules, ACME helps ensure responsible data handling and reduces risks associated with data breaches, unauthorized disclosure, and misuse of technology.

Scope

This policy applies to all employees, contractors, temporary workers, interns, and authorized third parties who access ACME systems or data. It applies to all digital assets, including cloud storage, email, messaging platforms, company websites, and internal systems. All individuals using ACME-owned or personally owned devices to access corporate resources must comply with this policy.

Data Classification Levels

ACME uses four data classification levels to determine the appropriate security controls and handling procedures required for different types of information.

1. **Public Data**
   Public data is information intended for broad external disclosure, such as marketing materials, job postings, and press releases. Unauthorized modification of public data may still pose risks; therefore, appropriate version control and publishing procedures must be followed.

2. **Internal Data**
   Internal data is restricted to ACME employees and approved third parties. Examples include internal communications, policies, project documentation, and departmental plans. Internal data requires basic safeguards such as restricted access and secure collaboration tools.

3. **Confidential Data**
   Confidential data includes sensitive business or customer information that requires elevated protection. Examples include customer order histories, employee performance

records, internal financial documents, and proprietary algorithms. Access to confidential data must be limited to authorized personnel based on business need.

4. **Restricted Data**
   Restricted data is the highest sensitivity level and includes personally identifiable information (PII), financial account numbers, health information, credentials, and security keys. Restricted data requires encryption, strict access controls, MFA, and enhanced monitoring. Employees handling restricted data must adhere to Policy 2’s IAM requirements and report any potential exposure immediately.

Data Privacy Requirements

ACME Corporation follows privacy-by-design principles to ensure that the collection and handling of personal information align with ethical and legal expectations. ACME collects only the minimum amount of personal data required for legitimate business purposes. This includes customer information needed to provide services and employee information required for workforce management.

Access to personal data must be restricted to authorized individuals with a demonstrated business need. Systems containing personal information must include auditing capabilities to track who accessed the data, when it was accessed, and for what purpose. Unauthorized viewing, copying, or sharing of personal information is strictly prohibited.

Data retention schedules must be followed to ensure personal data is not stored longer than necessary. When data is no longer needed, it must be securely deleted using approved disposal methods such as cryptographic erasure or secure document destruction.

Acceptable Use of ACME Technology

ACME’s technology resources—including computers, mobile devices, internet access, cloud platforms, software applications, and communication systems—must be used responsibly and only for authorized business purposes. Limited personal use is permitted as long as it does not interfere with daily operations, violate policy, or consume excessive system resources.

The following activities are prohibited:

- Accessing illegal, inappropriate, or harmful content

- Installing unauthorized software or connecting unapproved hardware

- Attempting to bypass security controls, firewalls, or monitoring systems
- Using ACME systems for personal business ventures, harassment, or fraudulent activity
- Sharing passwords or leaving devices unlocked while unattended
- Storing restricted data on unapproved personal devices or cloud services

Employees must report suspicious emails, phishing attempts, or unexpected pop-ups to the security team immediately. Failure to follow acceptable use guidelines may result in disciplinary action.

Monitoring and Privacy Expectations

Employees must understand that using ACME systems implies consent to monitoring. ACME regularly reviews logs, network traffic, email metadata, and device activity to ensure compliance with corporate policies and detect security incidents. ACME does not monitor personal content on personal devices beyond what is necessary for security if those devices access company systems.

Monitoring activities must remain minimally intrusive and limited to legitimate business and security purposes. Only authorized personnel such as IT, Security, and Human Resources may review monitoring data. Employees will be notified of significant monitoring changes when appropriate.

Data Retention and Disposal

To minimize exposure risks, ACME stores data only as long as necessary for business and compliance purposes. Although ACME does not model real-world regulatory frameworks within this college assignment scope, the following retention schedule applies for academic demonstration purposes:

- Routine email messages: 90 days
- Business communications: 1–3 years
- Personnel files: Duration of employment + 3 years
- Customer transaction data: Active relationship + 2 years

- System and security logs: Minimum 1 year

Data must be disposed of securely using approved methods such as shredding, secure deletion tools, or degaussing for magnetic media.

Relationship to Other Policies

This policy collaborates closely with the following:

- **Policy 1:** Security Architecture and data protection requirements
- **Policy 2:** Access restrictions for classified data
- **Policy 4:** Breach response involving personal or confidential information

---

Enforcement

Violations of this policy may result in disciplinary action, including access revocation, written warnings, suspension, or termination. Severe violations involving intentional misuse or data theft may result in legal consequences.

Policy 4: Incident Response and Business Continuity Policy

Purpose

The purpose of the Incident Response and Business Continuity Policy is to define how ACME Corporation identifies, reports, investigates, and recovers from cybersecurity incidents and service disruptions. A structured incident response approach helps minimize damage, restore operations quickly, protect sensitive information, and prevent recurrence.

Scope

This policy applies to all personnel and systems within ACME. Any employee who observes suspicious system behavior, receives a phishing attempt, or becomes aware of unauthorized access must follow the reporting procedures. This policy covers digital incidents, such as malware infections, unauthorized data access, system outages, and attempted compromise, as well as operational disruptions that may impact business continuity.

Incident Classification

ACME categorizes incidents into four severity levels:

- **Critical Incidents**: Ransomware attacks, ongoing data exfiltration, major service outages, or a confirmed breach of restricted data. These incidents demand immediate escalation to the CISO and executive leadership.

- **High Severity Incidents**: Unauthorized access to confidential systems, widespread malware, or system compromise affecting multiple users. These must be escalated within one hour.

- **Medium Severity Incidents**: Isolated malware, repeated suspicious login attempts, or minor policy violations with security implications.

- **Low Severity Incidents**: Minor misconfigurations, policy violations without confirmed compromise, or low-risk alerts requiring documentation but not urgent escalation.

Incident Reporting Requirements

Every employee is responsible for identifying and reporting suspicious activity. Incidents must be reported to the ACME Security Team through email, help desk ticket, or direct supervisor escalation. Reports must include a description of the issue, the affected systems, and the time the incident was detected. Prompt reporting ensures swift containment and reduces overall business impact.

Incident Response Phases

ACME follows a structured, step-by-step response model aligned with standard security frameworks:

1. **Identification**
   Determine whether an unusual event qualifies as an incident by analyzing logs, alerts, reports, or user observations.

2. **Containment**
   Temporarily isolate systems, disable compromised accounts, block suspicious IPs, or shut down infected devices to prevent further damage.

3. **Eradication**
   Remove malware, eliminate unauthorized access, close exploited vulnerabilities, and apply necessary patches.

4. **Recovery**
   Restore systems from backups, verify that vulnerabilities have been resolved, and bring systems back online in a controlled manner.

5. **Lessons Learned**
   Conduct post-incident analysis to identify root causes, document actions taken, and implement long-term improvements.

This structure helps ensure consistent handling of incidents and improves the overall maturity of ACME’s cybersecurity posture.

Evidence Handling

Proper evidence handling is essential when documenting incidents or supporting investigative needs. Logs, screenshots, system images, and user reports may be used as evidence. Employees must not alter system data or attempt to investigate incidents independently. Instead, all evidence must be preserved for security teams to analyze using approved tools and methods.

Business Continuity Essentials

ACME’s business continuity strategy ensures that critical operations can continue or resume quickly in the event of disruptions. Essential components include:

- Identification of critical systems and processes

- Backup strategies that protect sensitive data and restore essential services

- Designated personnel responsible for continuity actions
- Annual review and small-scale testing of business continuity plans

ACME prioritizes restoring services based on operational necessity, customer impact, and data sensitivity.

Relationship to Other Policies

Incident Response interacts closely with:

- **Policy 2:** Incident handling involving compromised identities
- **Policy 3:** Privacy implications and notifications
- **Policy 5:** Vulnerability exploitation, patch failure, or outdated systems

---

Enforcement

Failure to report incidents or comply with response actions may lead to disciplinary measures. Intentional interference with an investigation may result in severe consequences, including termination.

Policy 5: Vulnerability and Patch Management Policy

Purpose

The Vulnerability and Patch Management Policy establishes a consistent approach for identifying, assessing, and addressing security vulnerabilities in ACME systems. Proper patching and remediation are essential to minimizing exploitation risks and preserving system integrity. This policy ensures timely updates, prioritized remediation, and coordinated efforts across technical teams.

Scope

This policy applies to all ACME-managed hardware, software, servers, cloud instances, applications, and network devices. It applies to internal IT teams, system administrators, and external service providers responsible for maintaining ACME systems.

Asset Inventory Requirements

ACME must maintain a current inventory of hardware devices, installed software, operating systems, and cloud resources. Each asset must have an assigned owner responsible for verifying accuracy and ensuring updates occur. Inventories must be reviewed quarterly, with changes documented promptly.

Vulnerability Scanning Requirements

Regular vulnerability scanning identifies weaknesses that require remediation. ACME uses automated tools to scan systems using both authenticated and unauthenticated methods.

- **Internet-facing systems**: Scanned weekly for rapid detection of high-risk exposures
- **Internal systems**: Scanned monthly to identify outdated configurations or vulnerabilities
- **New deployments or changes**: Must be scanned within 24 hours

Scan results must be reviewed by security staff and assigned to appropriate owners for remediation.

Prioritization and Remediation Timelines

ACME prioritizes vulnerabilities based on severity, exposure, and potential business impact. Consistent with industry standards, the following remediation timelines apply:

- **Critical**: Remediate within 7 days
- **High**: Remediate within 14 days
- **Medium**: Remediate within 30 days

- **Low**: Remediate within 90 days

Exceptions require documented justification and approval from the system owner and security team.

Patch Management Requirements

Security updates must be tested and deployed in a structured manner:

- Testing ensures patches do not disrupt system functionality
- Emergency patches may be applied immediately during active threats
- Unsupported or outdated software must be upgraded or removed
- Administrators must verify successful installation and document patching results

Patch deployment schedules must align with vulnerability severity and operational needs.

Relationship to Other Policies

This policy interacts with:

- **Policy 1:** System architecture and baseline configurations
- **Policy 2:** Identity-related vulnerabilities and privileged account exposures
- **Policy 4:** Incident response actions when vulnerabilities are exploited

---

Enforcement

Failure to remediate vulnerabilities in accordance with this policy may lead to disciplinary measures, especially if negligence contributes to a security incident.