Information Security Policy

Acme Software Inc.

Document Type:	Written Information Security Program (WISP)
Effective Date:	August 27, 2025
Security Contact:	security@acme-compli.com
Review Schedule:	Every 12 months

1. Policy Overview

This Information Security Policy serves as the Written Information Security Program (WISP) for Acme Software Inc.. It establishes security standards and practices to protect company and customer information, ensure business continuity, and maintain trust. This policy applies to all employees, contractors, and third parties who access company systems or data. **Purpose:** This policy supports our compliance efforts and implements practical security controls appropriate for our business size and risk profile. We follow industry best practices and consider relevant regulatory requirements in our security approach. **Scope:** This policy covers information systems, data, communication channels, and facilities used in business operations. All personnel must understand and follow these security requirements.

2. Access Control & Authentication

Password Requirements: All staff must use strong, unique passwords. A password manager is required for all work accounts. **Multi-Factor Authentication:** Two-factor authentication (MFA) is required for all accounts. **Access Management:** User access follows the principle of least privilege. When employees leave the organization, all access must be removed within 24 hours. **Account Monitoring:** Regular reviews of user accounts and permissions are conducted to ensure appropriate access levels.

3. Device & Endpoint Security

All devices accessing company data must meet minimum security standards: • Personal devices may be used for work (BYOD policy in effect) • Disk encryption is required on all laptops (FileVault, BitLocker) • Automatic screen lock is required after idle periods • Operating system and application updates are required to be kept current **Device Management:** Company devices are configured with standard security baselines. Personal devices used for work must comply with our BYOD security requirements.

4. Network & Remote Work Security

Wi-Fi Security: Use secure Wi-Fi networks (WPA2/WPA3 encryption). Avoid unknown public networks for sensitive work. **Remote Work:** Remote work is supported with appropriate security controls. Employees must ensure secure network connections and maintain the same security standards as in-office work. **Network Monitoring:** Network traffic is monitored for security threats and policy compliance.

5. Email & Communication Security

Email Security Measures: • DMARC policy is configured: quarantine • Auto-forwarding to personal email accounts is prohibited • Suspicious emails should be reported to: security@acme-compli.com **Communication Guidelines:** Use approved communication platforms for business discussions. Be cautious with links and attachments from unknown senders. **Data Sharing:** Sensitive information should only be shared through approved, secure channels.

6. Data Protection & Privacy Controls

Data Classification: We use a standardized 4-level data classification system (Public, Internal, Confidential, Restricted): • **Public:** Information we can share openly • **Internal:** Information for internal use only • **Confidential:** Sensitive information like customer data and business secrets • **Restricted:** Highly sensitive information requiring special protection **Data Handling:** Data must be handled according to its classification: • Access limited to those who need it for their job • Encryption for sensitive data • Secure deletion when no longer needed • Keep data only as long as needed for business or legal reasons **Storage Requirements:** Work files cannot be stored in personal cloud accounts. Use approved business storage systems only. **Backups:** Critical business data must be backed up regularly and tested for recovery. **Encryption:** Sensitive data is protected using AES-256 encryption with key management procedures. This provides strong protection for sensitive data.

7. Risk Management & Business Continuity

Risk Assessment: We regularly review our security risks, typically annually or when major changes occur. This helps us focus our security efforts on the most important areas. **Business Impact**

Planning: We identify our most critical business functions and plan for how to maintain or quickly restore them if security incidents occur. **Risk Transfer:** We maintain cybersecurity insurance to help cover costs if major security incidents occur, including data breach response and business interruption.

8. Incident Response

What to Report: Report security incidents including data breaches, lost devices, malware, suspicious emails, or unauthorized access attempts. **How to Report:** Contact John Acme at ops@acme-compli.com within 16 hours. **Response Process:** We aim to contain critical incidents within 2 hours for critical incidents and follow a structured process: assess, contain, investigate, fix, recover, document, and notify as required. **Communication:** We will notify affected parties and authorities as required by law, typically within 72 hours for data breaches.

9. Vendor & Third-Party Management

Vendor Risk Assessment: Vendors handling Confidential data are required to undergo security assessments before engagement. **Data Processing Agreements:** Third-party processors must sign data protection addendums (DPAs) before processing company data. **Vendor Monitoring:** Regular reviews ensure ongoing compliance with security standards.

10. Security Training & Awareness

Training Schedule: Security awareness training is conducted Onboarding + Annual for all employees and contractors. **Training Content:** Covers current threats, company policies, incident reporting, and security best practices. **Compliance Tracking:** Training completion is tracked and reported to ensure 100% participation.

11. Policy Governance

Policy Owner: Security Officer **Review Schedule:** This policy is reviewed every 12 months or as needed based on business changes, security incidents, or regulatory updates. **Industry Frameworks:** This policy considers guidance from industry frameworks such as the NIST Cybersecurity Framework and other recognized security standards. **Employee Acknowledgment:** All employees must acknowledge receipt and understanding of this policy. Violations may result in disciplinary action up to and including termination.

This Written Information Security Program (WISP) demonstrates Acme Software Inc.'s commitment to protecting sensitive information through practical security controls and risk management practices.