Acme Corp - Security Overview

At Acme Corp, we are committed to maintaining a robust security and compliance posture. This document outlines our core practices, controls, and policies across information security, infrastructure, access control, and regulatory compliance.

1. Information Security Program

Acme Corp maintains an enterprise-wide information security policy aligned with ISO 27001 standards. The policy is reviewed annually and covers risk management, data handling, and user responsibilities.

2. Certifications and Compliance

We are ISO 27001 certified and conduct regular SOC 2 Type II audits. Compliance tracking includes GDPR, HIPAA, and CCPA.

3. Risk Management and Penetration Testing

Risk assessments are conducted quarterly. Independent penetration tests are performed at least once annually, with remediation tracked via Jira.

4. Employee Security Awareness

All employees undergo mandatory annual security training covering phishing, secure development, and acceptable use. Background checks are conducted for employees handling sensitive data.

5. Authentication and Access Control

We enforce multi-factor authentication (MFA) across all systems. Access is role-based and reviewed quarterly. A formal process exists for granting and revoking access.

6. Data Encryption

Sensitive data is encrypted at rest using AES-256 and in transit using TLS 1.3. Mobile devices and laptops are fully encrypted and remotely wipeable.

7. Logging and Monitoring

System activity and access logs are retained for at least 1 year. Logs are reviewed regularly for anomalies. Service accounts and administrative privileges are reviewed monthly.

8. Backups and Disaster Recovery

Backups are performed daily and tested monthly. Our disaster recovery plan is reviewed quarterly, and recovery point objectives (RPO) are under 4 hours.

9. Incident Response

Acme Corp maintains an incident response plan which is tested quarterly through tabletop exercises. A formal process is in place for internal reporting.

10. Physical and Network Security

Access to data centers is badge-controlled and logged. Network devices are hardened before deployment, and strong segmentation is enforced.

11. Secure Software Development

We follow a secure SDLC. All code is peer-reviewed, scanned for vulnerabilities, and deployed via CI/CD pipelines. Vulnerabilities are tracked until remediation.

12. Third-Party Risk

Vendors are reviewed annually for security compliance. All third-party tools must pass a security

review. Integrations are scoped and access-limited.

13. Endpoint and Email Security

Endpoints are protected by EDR software. We use a secure email gateway with phishing protection and optional encryption for sensitive communications.

14. Acceptable Use and Policies

An Acceptable Use Policy is signed by all employees. Systems enforce session timeouts, clock synchronization, and auto-logout for inactivity.

15. Technical Controls and Practices

Default credentials are changed on deployment. DLP tools monitor sensitive data movement. Production access is tightly restricted and logged.

16. Compliance and Audit

Internal security audits are conducted semi-annually. We track our adherence to relevant regulations and document all control evidence in a compliance portal.