ACME Corporation Company Policy (Data Security & Privacy Policy)

ACME CORPORATION

DATA SECURITY AND PRIVACY POLICY

Effective Date: January 1, 2024

SECTION 1: DATA CLASSIFICATION

1.1 All company data must be classified as Public, Internal, Confidential, or Restricted.

1.2 Restricted data includes: customer PII, financial records, trade secrets, and authentication credentials.

SECTION 2: DATA HANDLING REQUIREMENTS

2.1 Restricted data must be encrypted at rest using AES-256 or equivalent.

2.2 Restricted data transmission must use TLS 1.3 or higher.

2.3 Customer PII must not be stored in logs, error messages, or debug outputs.

2.4 All database queries containing PII must be parameterized to prevent SQL injection.

SECTION 3: ACCESS CONTROL

3.1 Access to Restricted data requires manager approval and must be reviewed quarterly.

3.2 All authentication must use multi-factor authentication (MFA).

3.3 API keys and credentials must be rotated every 90 days.

SECTION 4: DATA RETENTION

4.1 Customer data must be deleted within 30 days of account closure request.

4.2 Backup retention must not exceed 7 years.

SECTION 5: INCIDENT RESPONSE

5.1 Security incidents must be reported within 1 hour of discovery.

5.2 Data breaches affecting customer PII must be disclosed within 72 hours.

VIOLATIONS:

- CRITICAL: Unencrypted customer PII, hardcoded credentials
- HIGH: Missing MFA, SQL injection vulnerabilities
- MEDIUM: Expired API keys, incomplete access reviews
- LOW: Missing data classification labels