ACME CORPORATION

DATA SECURITY AND PRIVACY POLICY

Effective Date: January 1, 2024

Version: 2.0

SECTION 1: DATA CLASSIFICATION

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

1.2 Restricted data includes:

- Customer personally identifiable information (PII)
- Financial records and payment card data
- Trade secrets and proprietary algorithms
- Authentication credentials (passwords, API keys, tokens)

SECTION 2: DATA HANDLING REQUIREMENTS

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

2.2 Restricted data transmission must use TLS 1.3 or higher for all network communications.

2.3 Customer PII must NOT be stored in:

- Application logs
- Error messages
- Debug outputs
- Analytics platforms

2.4 All database queries containing PII or sensitive data must be parameterized to prevent SQL injection attacks.

2.5 API responses must not expose internal system details in error messages.

SECTION 3: ACCESS CONTROL

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

3.2 All authentication for systems handling Restricted data must use multi-factor authentication (MFA).

3.3 API keys and service credentials must be:

- Stored in secure secret management systems (not hardcoded)
- Rotated every 90 days maximum
- Revoked immediately upon employee departure

3.4 Service accounts must have minimum necessary privileges (principle of least privilege).

═══════════════════════════════════════

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 unless required by law.

4.3 Automated deletion processes must be implemented and tested quarterly.

4.4 Data deletion logs must be maintained for audit purposes.

═══════════════════════════════════════

SECTION 5: INCIDENT RESPONSE

═══════════════════════════════════════

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

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

5.3 All security incidents must be documented with:

- Timeline of discovery and response
- Root cause analysis
- Remediation steps taken

═══════════════════════════════════════

VIOLATION SEVERITY GUIDELINES:

═══════════════════════════════════════

🔴 CRITICAL (immediate remediation required):

- Unencrypted customer PII or financial data
- Hardcoded credentials (passwords, API keys, tokens)
- Active SQL injection vulnerabilities
- Missing encryption for data in transit

🟠 HIGH (remediation within 7 days):

- Missing MFA for sensitive systems
- SQL injection risk from poor coding practices
- Non-compliant data retention periods
- Improper PII handling in logs

🟡 MEDIUM (remediation within 30 days):

- Expired API keys (>90 days old)
- Incomplete quarterly access reviews
- Missing audit logging

🟢 LOW (remediation within 90 days):

- Missing data classification labels
- Incomplete documentation
- Minor process deviations

END OF POLICY DOCUMENT
