ACMECORP CLOUD SECURITY POLICY

Document ID: SEC-POL-001 | **Version:** 1.1 | **Date:** 13/2/2026
Owner: Fatima Nasir Muhammad, Security Team

1. PURPOSE

This policy establishes security requirements for all cloud services used by AcmeCorp, including Amazon Web Services (AWS) and Google Cloud Platform (GCP). It applies to all employees, contractors, and third parties with access to AcmeCorp cloud resources.

2. DATA CLASSIFICATION

- **PUBLIC:** Information approved for public release. No restrictions.
- **INTERNAL:** Information for internal use only. Not for public sharing.
- **CONFIDENTIAL:** Sensitive business information. Restricted access required. Must be encrypted.
- **RESTRICTED:** Highest sensitivity. PII, financial data, credentials. Encryption mandatory. Access logged.

3. ACCESS CONTROL REQUIREMENTS

- All cloud accounts must enforce **Multi-Factor Authentication (MFA)**. Ref: NIST AC-7
- Access must follow the **Principle of Least Privilege (PoLP)**. Users receive only the permissions needed. Ref: NIST AC-6
- Access must be reviewed quarterly and revoked when no longer needed. Ref: NIST AC-2
- Root/admin accounts must not be used for day-to-day operations.

4. CLOUD CONFIGURATION STANDARDS

- **S3 buckets must NOT be publicly accessible** unless explicitly approved by the Security team. Ref: NIST SC-7
- All data at rest must be encrypted. All data in transit must use **TLS 1.2+**. Ref: NIST SC-28, SC-8
- CloudTrail/Cloud Audit Logs must be enabled in all accounts at all times. Ref: NIST AU-2
- Security groups must follow a **default-deny posture**. Only explicitly approved ports may be open.

5. INCIDENT RESPONSE

All suspected security incidents must be reported to **security@acmecorp.com** within 1 hour of discovery. The Security team will follow the AcmeCorp Incident Response Plan (IRP-001). All incidents will be logged and reviewed. Ref: NIST IR-6

6. POLICY ENFORCEMENT & REVIEW

- **Enforcement:** Compliance with this policy is mandatory. Deviations must be documented as an exception and approved by the Security Lead. Non-compliance may result in disciplinary action or revocation of cloud access.
- **Review:** This policy will be reviewed annually or following any significant change to the cloud environment or applicable regulations