Cloud Security Policy

Purpose

This policy defines security requirements for cloud resources deployed across multiple regions to ensure confidentiality, integrity, and availability of systems and data.

Scope

Applies to all AWS accounts, services (EC2, S3, IAM), and users involved in deploying and maintaining the infrastructure in **US-East-1** and **EU-West-1** regions.

Policy

1. Identity & Access Management (IAM)

- All users must use **individual IAM accounts** (no shared credentials).
- Access must follow the **principle of least privilege**.
- **Multi-Factor Authentication (MFA)** is mandatory for root and IAM users.
- IAM roles must be used for EC2 instances, restricted to necessary actions only.

2. Compute (EC2 Instances)

- EC2 instances must only expose required ports:
    - **22 (SSH)** for administrators
    - **80 (HTTP)** for web traffic
- Security Groups must restrict SSH access to trusted IPs.
- Systems must be kept updated with the latest security patches.

3. Storage (S3 Buckets)

- S3 buckets must **block all public access**.
- **Encryption at rest (SSE-S3)** and **versioning** must be enabled.
- Logging must be enabled, with logs stored in a secure bucket.

4. Logging & Monitoring

- **CloudTrail** must log all management events across regions.
- Logs must be stored in encrypted, access-controlled S3 buckets.
- Monitoring alerts must be configured for unauthorized access attempts.

5. Compliance & Review

- Security configurations must be reviewed **quarterly**.
- Any deviation from this policy requires written approval from the security team.

Enforcement

Violations of this policy may result in revocation of access privileges, disciplinary action, or escalation to management.