Cloud Access Policy (CAP)

Organization Name: ClearTech Solutions

Policy Owner: IT Security Department

Policy Approval Date: April 4, 2025

Next Review Date: April 4, 2026

Policy Version: 1.0

1. Policy Objective

This Cloud Access Policy defines standards for accessing and managing cloud services (AWS, Azure, and Google Cloud) to ensure secure handling of organizational resources and data. It aims to reduce unauthorized access, protect against cloud-native threats, and enforce least privilege across all accounts.

2. Scope & Applicability

This policy applies to all employees, contractors, third-party vendors, and system accounts who access organizational cloud environments.

3. Definitions

- Cloud Provider – A third-party service offering cloud computing platforms (e.g., AWS, Azure).

- IAM (Identity and Access Management) – Policies and tools for ensuring the right individuals access the right resources.

- MFA (Multi-Factor Authentication) – A security mechanism requiring multiple forms of verification.

4. Policy Requirements

4.1 Identity & Access Management

- All users must be authenticated through federated identity or SSO.

- MFA is mandatory for all user logins.

- Default “root” or “owner” accounts must not be used for day-to-day operations.

4.2 Least Privilege

- Users and roles must be granted only the minimum permissions necessary.

- Access must be role-based (RBAC or ABAC), not user-based.

- Quarterly reviews must be conducted to remove stale or excessive permissions.

4.3 Logging & Monitoring

- All login and API access must be logged via native cloud tools (e.g., AWS CloudTrail, Azure Monitor).

- Logs must be stored securely for at least 180 days.

- Alerts must be triggered for anomalous behavior (e.g., location anomalies, excessive failed logins).

4.4 Cloud Resource Access

- Access to cloud consoles must only occur via secure, corporate-approved networks or VPN.

- Direct access to production resources must be restricted to authorized DevOps or Security Engineers.

- Access to storage (e.g., S3, Blob) must require encryption and access logs.

5. Roles and Responsibilities

- Cloud Security Team: Define IAM policies and monitor usage.

- IT Department: Implement and maintain access controls and audit tools.

- Users: Follow approved access procedures and report suspicious activity.

6. Enforcement

Violations of this policy may result in disciplinary action, including access revocation, reporting to HR, and possible termination.

7. References

- NIST SP 800-53: Access Control (AC) Controls

- CIS Benchmarks for AWS, Azure, GCP

- ISO/IEC 27001: A.9 – Access Control