GCP IAM Advanced Access Management Policy

1. Identity & Access Control Best Practices

- Implement Principle of Least Privilege (PoLP) across all roles.
- Use Google Groups for role assignments to simplify IAM management.
- Enforce Multi-Factor Authentication (MFA) for all privileged accounts.
- Regularly audit IAM policies and remove unused permissions.

2. Service Accounts & Key Management

- Rotate service account keys every 90 days to reduce risk exposure.
- Restrict service accounts to specific VPC networks for enhanced security.
- Use Workload Identity Federation to minimize key usage.

3. Custom Roles & Audit Logs

- Create custom roles instead of using primitive roles (Owner, Editor, Viewer).
- Enable Cloud Audit Logs to capture IAM policy changes.
- Use BigQuery for long-term storage and analysis of IAM audit logs.