Google Cloud Security Policy

1. Purpose

This policy establishes security requirements for the use of Google Cloud Platform (GCP) to protect organizational data, programs, and framework from unauthorized access, breaches, and other cyber threats.

2. Scope

This policy applies to all employees, contractors, and third parties using GCP services, including Compute Engine, Cloud Storage, BigQuery, Kubernetes Engine, and other GCP resources.

3. Security Principles

- **Least Privilege Access:** Users and services should only have minimum permissions necessary.
- **Zero Trust Model:** Verification of user and device identity.
- **Defense-in-Depth:** Layered security measures to reduce attack surfaces.
- **Encryption First:** All data should be encrypted at rest and in transit.
- **Compliance & Governance:** Adhere to regulatory requirements such as GDPR, HIPAA, and ISO 27001.

4. Identity & Access Management (IAM)

- Use Google Cloud IAM roles with principle of least privilege.
- Enable multi-factor authentication (MFA) for user accounts.
- Use Cloud Identity-Aware Proxy (IAP) to secure access to applications.
- Enforce service account key rotation and limit direct key access.
- Regularly review IAM roles and remove inactive accounts.

5. Data Security

- Code all data at rest using Google-managed encryption keys or Customer-Managed Encryption Keys (CMEK).
- Encrypt data in transit using TLS 1.2 or higher.
- Use VPC Service Controls to restrict data movement.
- Allow Cloud DLP (Data Loss Prevention) to detect and redact sensitive information.
- Apply Object Lifecycle Policies to automate data retention and deletion.

6. Network Security

- Use Virtual Private Cloud (VPC) with firewall rules to restrict traffic.
- Enable Cloud Armor for DDoS protection.
- Use Private Google Access to prevent public internet exposure.
- Enforce Identity-Aware Proxy (IAP) for remote access.
- Monitor network logs with VPC Flow Logs and Cloud Logging.

7. Security Monitoring & Incident Response

- Authorize Cloud Logging and Cloud Monitoring to track activity.
- Use Security Command Center for threat detection.
- Structure SIEM integration (e.g., Chronicle, Splunk).
- Run security alerts using Cloud Pub/Sub and Cloud Functions.
- Create an incident response plan with clear escalation paths.

8. Application Security

- Utilize Cloud Build with security scanning to detect vulnerabilities.
- Apply Cloud Run & Kubernetes security best practices.
- Allow API Gateway with authentication and rate limiting.
- Use Web Security Scanner to identify application vulnerabilities.

9. Compliance & Auditing

- Run regular security audits and penetration testing.
- Use Access Transparency Logs to monitor Google's administrative access.
- Maintain audit logs using Cloud Audit Logging.
- Certify compliance with industry standards (e.g., ISO 27001, SOC 2).

10. Backup & Disaster Recovery

- Use Cloud Storage Bucket Versioning to protect against data loss.
- Perform backups with Cloud SQL Backup & Restore.
- Ensure cross-region redundancy for disaster recovery.
- Regular backup testing to verify integrity.

11. Third-Party & Supply Chain Security

- Use third-party applications and services for security compliance.
- Enforce service-level agreements (SLAs) for cloud vendors.
- Use BeyondCorp Enterprise for secure access to third-party tools.

12. Enforcement & Penalties

- Violations to this policy may result in provoked access, disciplinary action, or legal action.
- Employees and contractors must partake in annual security training.