GCP Data Protection & Encryption Policy

1. Data Classification & Sensitivity Levels

- Categorize data into Public, Internal, Confidential, and Restricted levels.

- Enforce automatic tagging of sensitive data using Cloud DLP.

2. Encryption Mechanisms

- Use Google-managed encryption keys for low-risk data.

- Require Customer-Managed Encryption Keys (CMEK) for high-risk data.

- Implement envelope encryption for an additional layer of security.

3. Data Loss Prevention (DLP)

- Enable Cloud DLP to detect and mask Personally Identifiable Information (PII).

- Use VPC Service Controls to prevent unauthorized data exfiltration.

- Implement Google Access Transparency Logs to monitor Google?s access to data.

4. Secure Data Storage

- Enforce Cloud Storage Bucket Policies to restrict access based on identity.

- Enable Object Versioning to track modifications and prevent accidental deletions.