# Architectural Decisions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID: | Subject: | Issue / Requirement: | Decision: | Rationale: | Source: Project Phase: |
| G06 | Folder/Project Structure | Need to define a scalable structure for organizing GCP resources aligned with departments or environments. Avoid project sprawl and ensure clear ownership. | Implement a GCP folder hierarchy under the Organization node, grouped by function (e.g., Production, Dev), and further by department. Each workload gets its own project. | Improves manageability, billing clarity, and policy enforcement by aligning GCP resources with organizational structure. |  |
| G07 | Network Architecture | Need to connect multiple projects securely and consistently while maintaining scalability and isolation. | Adopt a hub-and-spoke network model using Shared VPCs. Centralized networking in the hub; departments connect via spokes. | Provides consistent security policies, centralized logging, and simplifies cross-project communication and control. |  |
| G08 | Firewall Strategy | Determine whether to use GCP-native firewall or third-party like Palo Alto for different workloads including IaaS and SaaS platforms. | Use GCP-native firewalls for standard workloads and integrate Palo Alto firewall appliances for high-security workloads. | Balances ease of use and cost efficiency with advanced threat protection for sensitive applications. |  |
| G09 | Identity and Access Management (IAM) | Need to integrate GCP IAM with MTA’s existing identity provider (Azure AD) for single sign-on and centralized user control. | Federate GCP with Azure AD using SAML. Leverage Google Cloud IAM roles with conditional access policies. | Supports enterprise-wide identity strategy, ensures secure and compliant access to GCP resources, and simplifies user lifecycle management. |  |