# Organization Policy Baseline – IAM & Network Security Hardening

Project: IAM & Network Security Hardening

Coverage: Weeks 1–2 — Foundational GCP Org Policies and Governance Controls

## 1. Overview

The Organization Policy Baseline defines mandatory governance constraints and configuration standards to ensure all Google Cloud resources align with security and compliance requirements. These policies enforce least privilege, resource boundaries, and data protection principles across all projects.

## 2. Enforced Organization Policies

|  |  |  |  |
| --- | --- | --- | --- |
| Policy Name | Constraint ID / Description | Applied Scope | Purpose |
| Disable Serial Port Access | constraints/compute.disableSerialPortAccess | All Compute Engine Instances | Prevents external serial port connections to VM instances. |
| Restrict External IPs | constraints/compute.vmExternalIpAccess | All Projects | Ensures internal workloads remain private and protected from internet exposure. |
| Enforce VPC Flow Logs | constraints/compute.requireVPCFlowLogs | All Networks | Captures network traffic metadata for monitoring and anomaly detection. |
| Restrict Service Account Key Creation | constraints/iam.disableServiceAccountKeyCreation | All Service Accounts | Prevents creation of long-lived keys to enforce Workload Identity Federation. |
| Domain Restricted Sharing | constraints/iam.allowedPolicyMemberDomains | Organization Level | Limits IAM role assignments to corporate domain members only. |
| Restrict Resource Locations | constraints/gcp.resourceLocations | All Projects | Restricts resource creation to US regions for compliance and data residency. |
| Disable Default Network Creation | constraints/compute.skipDefaultNetworkCreation | Organization Level | Ensures new projects do not have a default, flat network that bypasses segmentation. |
| Require OS Login | constraints/compute.requireOsLogin | All VMs | Forces IAM-based SSH access control instead of static SSH keys. |
| Restrict Public Buckets | constraints/storage.uniformBucketLevelAccess | All Cloud Storage Buckets | Applies uniform IAM policies and prevents anonymous access to storage objects. |
| Require CMEK for Data Storage | constraints/sql.restrictAuthorizedNetworks | Cloud SQL and Storage | Mandates encryption with Customer-Managed Encryption Keys (CMEK). |

## 3. Compliance Alignment

These organization policies map directly to NIST CSF and CIS GCP controls:  
• NIST PR.AC-1, PR.AC-3 – Access Control and Least Privilege  
• NIST PR.DS-1 – Data Security and Encryption  
• CIS GCP 1.1–1.8 – IAM and Resource Governance  
• CIS GCP 3.1–3.4 – Network Security  
• CIS GCP 6.1–6.3 – Data Protection and Storage

## 4. Governance & Exception Process

All enforced policies are managed by the Organization Admin team under the Security Lead’s supervision. Requests for exceptions must be formally submitted via a Change Request (CR) with a documented business justification. Each exception must specify duration, compensating controls, and be approved by the Project Sponsor.

## 5. Audit & Monitoring

• Weekly audit of organization policy violations through Security Command Center findings.  
• Automated policy compliance checks via Cloud Asset Inventory and Cloud Config Validator.  
• Policy updates tracked via version-controlled Terraform modules.  
• Quarterly policy review meetings to update constraints based on evolving GCP best practices.