Policy Enforcement Document: constraints/storage.secureHttpTransport

# 1. Overview: What is constraints/storage.secureHttpTransport?

* • The constraints/storage.secureHttpTransport is an Organization Policy Constraint in Google Cloud that enforces secure communication to and from Cloud Storage buckets.
* • This policy denies any unencrypted (HTTP) traffic to buckets.
* • Helps in preventing man-in-the-middle attacks by requiring encryption in transit.
* • Enforces data protection best practices aligned with compliance requirements (e.g., PCI-DSS, ISO 27001).
* • Once enforced, all HTTP requests will be rejected with an error.

# 2. What Are We Changing?

* • Enforcing constraints/storage.secureHttpTransport = TRUE across all projects.
* • Blocking any public or internal access over HTTP to GCS buckets.
* • Auditing existing applications/scripts for HTTP usage and updating them.
* • Updating project policies to comply with this constraint.
* • Ensuring future resources default to secure communication practices.

# 3. Why Are We Changing This?

* • Prevent data leakage during transit by disallowing unencrypted access.
* • Mitigate security risks such as interception or tampering.
* • Align with regulatory and compliance frameworks.
* • Meet internal security and audit requirements.
* • Strengthen Zero Trust Architecture (ZTA) principles in the cloud environment.

# 4. Actions for the Project Team

* • Audit applications, tools, or scripts using HTTP and update to HTTPS.
* • Validate third-party tools or services interacting with GCS use HTTPS.
* • Update internal documentation or onboarding guides to reflect this policy.
* • Communicate the change to developers and DevOps engineers.
* • Verify all Cloud Storage requests post-change to ensure continuity.

# 5. Important Considerations

* • Projects using HTTP will experience request failures post-enforcement.
* • The policy is non-reversible without explicit exception approval.
* • Bucket-level configurations cannot override this organization policy.
* • Exemptions must be requested and justified through the Security Council.
* • Violations may result in non-compliance flags during audits or security reviews.