# IAM Policy Document – ShopNimbus Security Project

\*\*Project ID:\*\* shopnimbus-security-group7

\*\*Prepared by:\*\* Gloria Akhadelor-Job

\*\*Date:\*\* October 12, 2025

## 1. Purpose

This IAM Policy Document defines the access management framework applied within the ShopNimbus Security Project. The purpose is to enforce the principle of least privilege by assigning specific roles to service accounts and users, ensuring controlled access to compute, storage, database, and encryption resources in compliance with NIST, CIS, and PCI DSS standards.

## 2. Scope

This policy applies to all users, service accounts, and automated processes operating within the Google Cloud Platform project ‘shopnimbus-security-group7’. It governs IAM configurations, permissions, and policy bindings for the Web, Application, and Database tiers.

## 3. IAM Roles and Service Accounts

The following roles were assigned to service accounts to enable secure operations while maintaining minimal privileges.

|  |  |  |  |
| --- | --- | --- | --- |
| Service Account / User | Role | Purpose | Access Scope |
| web-sa@shopnimbus-security-group7.iam.gserviceaccount.com | roles/compute.viewer | View compute instances and firewall configuration | Web Tier |
| app-sa@shopnimbus-security-group7.iam.gserviceaccount.com | roles/cloudsql.client | Permit secure connections to Cloud SQL instance | Application Tier |
| database-sa@shopnimbus-security-group7.iam.gserviceaccount.com | roles/cloudkms.cryptoKeyEncrypterDecrypter | Allow encryption and decryption of stored data | Database Tier |
| service-363546819737@gcp-sa-logging.iam.gserviceaccount.com | roles/bigquery.dataEditor | Write Security Command Center findings to BigQuery | Centralized Logging |
| gloria@shopnimbus-security-group7 | roles/owner | Administrative and audit oversight | Project Level |

## 4. Commands Executed

Commands executed to create and bind roles:  
gcloud iam service-accounts create web-sa --display-name='Web Tier Service Account'  
gcloud iam service-accounts create app-sa --display-name='App Tier Service Account'  
gcloud iam service-accounts create database-sa --display-name='Database Tier Service Account'  
  
gcloud projects add-iam-policy-binding shopnimbus-security-group7 --member='serviceAccount:web-sa@shopnimbus-security-group7.iam.gserviceaccount.com' --role='roles/compute.viewer'  
gcloud projects add-iam-policy-binding shopnimbus-security-group7 --member='serviceAccount:app-sa@shopnimbus-security-group7.iam.gserviceaccount.com' --role='roles/cloudsql.client'  
gcloud projects add-iam-policy-binding shopnimbus-security-group7 --member='serviceAccount:database-sa@shopnimbus-security-group7.iam.gserviceaccount.com' --role='roles/cloudkms.cryptoKeyEncrypterDecrypter'

## 5. Verification Commands

Verification commands were executed to confirm IAM policy bindings and role propagation:  
gcloud projects get-iam-policy shopnimbus-security-group7 --format='table(bindings.role, bindings.members)'  
gcloud iam service-accounts list

## 6. Compliance References

- NIST PR.AC-1: Identities and credentials are issued and managed for authorized devices and users.  
- NIST PR.AC-4: Access permissions are managed through IAM role assignments.  
- CIS Control 5: Securely configure and manage access control for cloud environments.  
- PCI DSS 7.1: Restrict access to system components and cardholder data by business need-to-know.

## 7. Policy Review and Maintenance

IAM policies will be reviewed quarterly to ensure ongoing compliance and least-privilege enforcement. Any new services added to the project must undergo a security impact assessment prior to IAM binding approval.