# ShopNimbus Cloud Security Hardening Project – Change Management and IaC Policy

Week 2 Deliverable – Governance and Compliance Phase

## 1. Purpose

The purpose of this policy is to define the standards and procedures for managing infrastructure and configuration changes within the ShopNimbus Cloud Security Hardening Project. It ensures all changes are controlled, documented, peer-reviewed, and auditable to maintain system security, stability, and compliance across Google Cloud environments.

## 2. Scope

This policy applies to all Google Cloud projects and environments under the ShopNimbus ecosystem, including Compute Engine, Cloud SQL, Cloud Functions, and Cloud Storage. It governs any changes made through Infrastructure-as-Code (IaC) using Terraform or direct configuration updates within the GCP console. The scope includes DevOps Engineers, Network Engineers, Security Leads, and the Project Sponsor.

## 3. Policy Statement

All infrastructure or configuration changes must be version-controlled, reviewed, approved, validated, and logged. Peer review and validation are required prior to deployment. Emergency changes may be implemented immediately but must undergo retrospective review and approval within 24 hours.

## 4. Change Workflow and Approval Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Change Type | Approvers / Reviewers | Validation Tool | Evidence / Log Location | Rollback Plan | Status |
| Terraform IaC Update (VPC, IAM, Firewall) | DevOps Engineer → Security Lead | Terraform Plan + Config Validator | GitHub Pull Request + BigQuery Audit Table | ‘terraform destroy’ rollback file | Active |
| Org Policy Update | Security Lead → Project Sponsor | Policy Analyzer | GCP Audit Logs / Drive | Previous policy JSON backup | Active |
| IAM Role Change | IAM Engineer → Security Lead | IAM Recommender | IAM Analyzer Logs / Drive | Revert to previous role binding | Active |
| Network Rule Modification | Network Engineer → Security Lead | Config Validator | SCC Network Findings Export | Restore prior VPC firewall config | Active |
| Emergency Fix / Patch | DevOps Engineer → Project Sponsor | Manual Review | SCC Logs / PR Audit | Post-change peer review within 24 hrs | Planned (Week 4) |

## 5. Version Control Policy

All Infrastructure-as-Code (IaC) configurations must be stored in GitHub with enforced branch protection rules. Pull Requests (PRs) must receive at least one approval from a Security Lead or DevOps Engineer prior to merge. Commit history will serve as the immutable audit trail. Drift detection and rollback mechanisms are implemented via Terraform plan/apply cycles. Any secrets must be managed through Google Secret Manager.

## 6. Compliance Alignment

|  |  |
| --- | --- |
| Framework / Regulation | Relevant Control |
| NIST CSF | PR.IP-3 – Configuration change control processes established |
| CIS GCP | 1.6, 3.1 – Infrastructure-as-Code and configuration management best practices |
| PCI DSS | 6.4.5 – Change control procedures documented and approved |
| GDPR | Article 32 – Security of processing and resilience of systems |

## 7. Evidence Management Note

All change management evidence — including Terraform plan outputs, approval logs, and configuration validation results — will be stored in the centralized audit repository. Evidence sources include GitHub (Pull Request history), BigQuery (audit logs), and Google Drive (policy backups). Screenshots and configuration diffs will be added during Week 4–5 validation when tool activation is complete. This ensures every infrastructure change can be traced, reviewed, and reproduced for audit or compliance verification under NIST PR.IP-3 and PCI DSS 6.4.5.