# ShopNimbus Cloud Security Hardening Project – Information Security Policy Suite

Week 1–2 Deliverable – Governance and Control Phase

## Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date / Phase | Prepared By |
| 1.0 | Week 1–2 Deliverable | Security Lead – ShopNimbus Project |

## 1. Access Control Policy

Purpose: To ensure least privilege and secure access to all ShopNimbus systems.  
Policy Summary:  
- All access must follow least-privilege and role-based principles.  
- MFA is required for all user and service accounts.  
- Access reviews occur quarterly using IAM Analyzer and SCC.  
- Service accounts may not use user-managed keys; all identities are centrally managed.  
Framework Links: NIST PR.AC-1, CIS 1.6, PCI DSS 7.1, GDPR Art. 32.

## 2. Network Security Policy

Purpose: To maintain secure network segmentation between the web, app, and database tiers.  
Policy Summary:  
- VPC firewalls and Cloud Armor WAF enforce boundary control.  
- Subnets separate public (web) from private (app and database) layers.  
- Only HTTPS (TLS 1.3) is allowed for inbound traffic.  
- Network logging (VPC Flow Logs) and SCC scanning monitor traffic integrity.  
Framework Links: NIST PR.PT-4, CIS 3.3, PCI DSS 1.3, GDPR Art. 32.

## 3. Data Retention & Privacy Policy

Purpose: To ensure compliance with data protection and retention standards (GDPR & PCI).  
Policy Summary:  
- Sensitive data (PII, PCI) must be encrypted at rest and in transit (CMEK + TLS).  
- Data is retained only for business and compliance needs.  
- Lifecycle rules automatically delete or archive inactive data after 12 months.  
- DLP scanning is used to detect and prevent sensitive data leaks.  
Framework Links: GDPR Art. 5(1)(e), GDPR Art. 32, PCI DSS 3.2, NIST PR.DS-5.

## 4. Vulnerability Management Policy

Purpose: To detect, assess, and remediate security vulnerabilities across cloud resources.  
Policy Summary:  
- Automated scans using Security Command Center (SCC) and Security Health Analytics occur weekly.  
- Findings must be reviewed within 5 business days.  
- Critical vulnerabilities must be remediated or mitigated within 72 hours.  
- Monthly reports summarize findings, trends, and actions taken.  
Framework Links: NIST DE.CM-7, CIS 2.3, PCI DSS 11.2, GDPR Art. 32.

## 5. Evidence Management Note

Evidence for compliance verification will be maintained in a centralized repository (Google Drive, BigQuery, SCC reports). Each policy is reviewed annually or after major system changes. Logs and reports will be validated in Week 4–5 once automation and monitoring are fully implemented. This ensures continuous compliance readiness and audit traceability.