Retail Bank PCI DSS Compliance Policy

Document Version: 1.0
Effective Date: [Insert Date]
Owner: Chief Information Security Officer (CISO)
Approved By: Board of Directors / Risk and Compliance Committee
Review Cycle: Annually or upon significant changes

---

1. Purpose

This policy establishes the framework by which [Retail Bank Name] ensures compliance with the **Payment Card Industry Data Security Standard (PCI DSS)**. It defines the scope, roles, processes, and controls necessary to protect cardholder data and maintain PCI DSS compliance across the organization.

---

2. Scope

This policy applies to all systems, personnel, and processes involved in storing, processing, or transmitting cardholder data (CHD) or sensitive authentication data (SAD). This includes, but is not limited to:

- **Internal Systems**: Core banking platforms, ATMs, POS systems, online/mobile banking, data centers
- **Third Parties**: Payment processors, cloud service providers, vendors with access to CHD
- **Staff**: All employees, contractors, and third-party personnel handling CHD

---

3. Scope Definition Process

To maintain a clear and accurate PCI DSS compliance scope, the following actions are mandated:

3.1 Asset and Data Flow Identification

- Inventory all systems that store, process, or transmit CHD
- Map data flows of CHD across networks, systems, and service providers
- Maintain up-to-date network diagrams with segmentation boundaries

3.2 Segmentation and Isolation

- Apply segmentation techniques to isolate the Cardholder Data Environment (CDE)

- Validate segmentation using penetration testing and firewall configuration reviews

---

4. Gap Analysis

A comprehensive gap analysis must be conducted at least annually or upon major system changes:

4.1 Assessment Process

- Compare current security controls against all 12 PCI DSS requirement domains
- Perform assessments internally or in collaboration with a Qualified Security Assessor (QSA)

4.2 Risk-Based Remediation

- Classify and prioritize identified gaps based on impact and exploitability
- Document and assign remediation tasks to responsible teams

4.3 Documentation

- Maintain a Gap Analysis Report detailing:
    - Compliance status of each PCI DSS requirement
    - Identified risks and vulnerabilities
    - Proposed corrective actions

---

5. Implementation Roadmap

The roadmap outlines structured phases for achieving and maintaining PCI DSS compliance:

5.1 Phase 1: Planning and Design

- Confirm compliance scope
- Define remediation plan and responsible owners
- Design updated network and control architecture

5.2 Phase 2: Remediation Activities

- Implement or enhance:
    - Access controls and MFA
    - Encryption mechanisms
    - Logging and monitoring tools

    - Security awareness training
- Update security policies and operational procedures

5.3 Phase 3: Testing and Validation

- Conduct:
    - Quarterly vulnerability scans
    - Annual internal and external penetration testing
    - Configuration reviews and access control verifications

5.4 Phase 4: Documentation and Certification

- Prepare necessary documentation (RoC, SAQ, AOC)
- Engage QSA (if applicable) for independent assessment and validation
- Submit compliance documentation to card brands/acquirers as required

---

6. Ongoing Maintenance and Governance

Maintaining compliance is a continuous effort requiring robust monitoring, assessment, and policy enforcement.

6.1 Monitoring and Logging

- Implement SIEM for real-time monitoring
- Monitor access to CDE and generate daily audit logs
- Apply File Integrity Monitoring (FIM) for sensitive systems

6.2 Regular Assessments

- Quarterly vulnerability scans (internal and ASV-certified external)
- Annual risk assessments
- Annual review of policies and procedures

6.3 Change Management

- Assess security impact of all changes affecting the CDE
- Update documentation and revalidate controls post-change

6.4 Security Awareness and Training

- Provide mandatory annual PCI DSS training to all relevant personnel
- Conduct periodic phishing simulations and social engineering drills

---

7. Roles and Responsibilities

Role	Responsibilities
CISO	Owns and oversees PCI DSS program; reports to Executive Committee
PCI Compliance Officer	Coordinates audits, gap analysis, remediation, and documentation
IT Security Team	Implements and monitors technical controls
Internal Audit	Independently validates compliance through internal reviews
Business Units	Ensure adherence to PCI requirements in daily operations

---

8. Enforcement

Non-compliance with this policy may result in disciplinary action, including revocation of access rights or termination. Contractual penalties may apply to third parties failing to meet PCI obligations.

---

9. References

- PCI DSS v4.0 Standard – https://www.pcisecuritystandards.org
- Retail Bank's Information Security Policy
- Data Protection and Privacy Policy
- Vendor Management Policy

---

10. Review and Revision

This policy shall be reviewed annually or upon major changes to systems, processes, or PCI DSS versions. Revisions must be approved by the Risk and Compliance Committee.

Document History

Version	Date	Description	Author
1.0	[Insert Date]	Initial draft	[CISO Name]