NB-71-25

# PCI DSS Information Security Policy

| Policy Owner | Chief Information Security Officer (CISO) |
|---|---|
| Effective Date | September 10, 2025 |
| Next Review Date | September 2026 |
| Classification | Internal Use Only |

## 1. Purpose

This policy defines the technical, physical, and administrative safeguards Northbridge must implement to comply with the Payment Card Industry Data Security Standard (PCI DSS). It ensures protection of cardholder data (CHD) and sensitive authentication data (SAD) against unauthorized access, theft, or misuse.

## 2. Scope

Applies to all systems, networks, and devices that store, process, or transmit cardholder data; all employees, contractors, and service providers with access to payment systems; and cloud or vendor-hosted environments handling CHD on behalf of Northbridge.

## 3. PCI DSS Security Control Requirements

3.1 Network Security
- Maintain and configure firewalls to protect cardholder data.
- Segregate cardholder data environments (CDE) from other corporate networks.
- Prohibit vendor default passwords; enforce strong configuration baselines.

3.2 Cardholder Data Protection
- Encryption at Rest: Cardholder data must be encrypted using strong algorithms (AES-256).
- Encryption in Transit: Data transmitted over open/public networks must use TLS 1.2+.
- Never store sensitive authentication data (full magnetic stripe, CVV, PIN blocks) after authorization.

3.3 Access Control
- Enforce least privilege access to cardholder data.
- Require Multi-Factor Authentication (MFA) for administrative and remote access.
- Assign unique IDs to all users; no shared accounts permitted.
- Role-based access reviews conducted quarterly.

3.4 Monitoring & Logging
- Log all access to cardholder data, including failed attempts.
- Centralize logs in a SIEM; retain for at least one year.
- Daily review of critical event logs (firewall, IDS/IPS, authentication events).

3.5 Vulnerability Management

- Apply critical security patches within 30 days of release (critical patches within 7 days).
- Perform internal vulnerability scans quarterly; external scans by Approved Scanning Vendor (ASV).
- Conduct penetration testing annually and after significant network changes.

3.6 Endpoint & System Security
- Anti-malware software must be deployed and updated daily.
- Secure configuration standards applied to all systems (CIS or vendor benchmarks).
- File integrity monitoring (FIM) deployed on critical systems.

3.7 Data Retention & Disposal
- Retain cardholder data only as long as required for business or legal reasons.
- Securely delete or destroy CHD when no longer needed (shredding, DOD wipe, or cryptographic erase).

3.8 Incident Response
- Maintain an Incident Response Plan specific to payment card data.
- Report suspected cardholder data breaches immediately to IT Security.
- Preserve forensic evidence and follow PCI Forensic Investigator (PFI) procedures.

## 4. Breach Risk Determination

- Encrypted CHD Compromise: If properly encrypted with strong keys, not considered a reportable PCI breach.
- Unencrypted CHD Compromise: Presumed PCI DSS violation; requires notification to acquiring bank, card brands, and regulators.
- Failure to Monitor or Patch: Increases risk rating and may result in fines.

## 5. Responsibilities

- CISO: Maintains this policy, reports compliance to executive leadership.
- IT Security: Implements firewalls, encryption, logging, monitoring, and vulnerability scans.
- System Owners: Ensure applications storing or processing CHD comply with PCI DSS.
- Employees: Must not store, email, or transmit cardholder data insecurely.

## 6. Enforcement

Non-compliant systems may be removed from the network. Violations may result in disciplinary action or termination. Vendors failing PCI DSS requirements may be terminated as service providers.