PCI DSS Responsibility Matrix

January 2025

Table of Contents

Revisions

Versions	Date	Description	Author	Approved By
0.1	2/1/2025	PCI DSS V4.0.1 Version Created	Kevin Burns	Draft
0.2	2/10/2025	Published for review	Kevin Burns	Stuart Andrew
0.3	2/12/2025	Reviewer updates	Kevin Burns	Gary Dahmer
1.0	2/13/2025	Published reviewed version	Kevin Burns	Ademola Obasola

Scope

This document outlines the Roles and Responsibilities of NMI, our Partners and our Merchants with respect to the controls in Version 4.x (currently v4.0.1) of the Payment Card Industry Data Security Standards (PCI DSS). The Controls apply to the NMI Card Payment Processing (Gateway) products including NMI ONE, Cardease, OMNI and USAePay as well as those NMI products which facilitate Card Payments including Merchant Central, ScanX and TransactionIntel. The NMI P2PE / E2EE solutions have a separate matrix due to the design and delivery of that specific solution type. For more details on requirements and testing procedures, search for the full PCI DSS v4.0.1 Standard at **https://www.pcisecuritystandards.org/document_library/**.

Responsible Party

As a general principle, NMI is responsible for all cardholder data which is stored, transmitted or processed within its environment. NMI is not responsible for cardholder data outside of its environment and this sits with the Partner or Merchant.

This matrix identified which party is responsible for a Control. Responsibility can be:	
X	This control is relevant
?	This control may be relevant

List of Acronyms

CDE	Cardholder Data Environment
CHD	Cardholder Data
DSS	Data Security Standard
E2EE	End to End Encryption
PAN	Primary Account Number

PCI	Payment Card Industry
PIM	P2PE Instruction Manual
P2PE	Point to Point Encryption
SAD	Sensitive Authentication Data
TRA	Targeted Risk Assessment

NMI P2PE / E2EE Responsibilities Matrix

Requirement	NMI	Partner	Merchant	Notes
	Party Responsible			
Requirement 1 - Install and Maintain Network Security	X			Assumes implementation follows the provided NMI P2PE PIM and the solution is not modified by the Partner or Merchant.
Requirement 2 - Apply Secure Configurations to All System Components	X			
Requirement 3 - Protect Stored Account Data	X			
Requirement 4 - Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	X			
Requirement 5 - Protect All Systems and Networks from Malicious Software	X			
Requirement 6 - Develop and Maintain Secure Systems and Software	X			
Requirement 7 - Restrict Access to System Components and Cardholder Data by Business Need to Know	X			
Requirement 8 - Identify Users and Authenticate Access to System Components	X			
Requirement 9 - Restrict Physical Access to Cardholder Data	X		X	
Requirement 10 - Log and Monitor All Access to System Components and Cardholder Data	X			
Requirement 11 - Test Security of Systems and Networks Regularly	X			
Requirement 12 - Support Information Security with Organizational Policies and Programs	X			

NMI PCI DSS Responsibilities Matrix

Requirement	NMI	Partial	Joint	All	N/A	Notes
	Party Responsible					
Requirement 1 - Install and Maintain Network Security						Each requirement is broken out into a number of controls which have been assessed in more detail to derive this summary.
Requirement 2 - Apply Secure Configurations to All System Components		X		X		
Requirement 3 - Protect Stored Account Data	X					
Requirement 4 - Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	X	?	?			
Requirement 5 - Protect All Systems and Networks from Malicious Software	X	?	?			
Requirement 6 - Develop and Maintain Secure Systems and Software	X	?	?			
Requirement 7 - Restrict Access to System Components and Cardholder Data by Business Need to Know	X	?	?			
Requirement 8 - Identify Users and Authenticate Access to System Components	X	?	?			
Requirement 9 - Restrict Physical Access to Cardholder Data				X		
Requirement 10 - Log and Monitor All Access to System Components and Cardholder Data	X					
Requirement 11 - Test Security of Systems and Networks Regularly	X	?	?			
Requirement 12 - Support Information Security with Organizational Policies and Programs				X		
Appendicies A1, A2, A3					X	Do not apply to NMI and not expected to apply to Partners or Merchants.

Requirement 1 - Install and Maintain Network Security Controls

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.	X	X	X	Each party is expected to maintain their own network security documentation.
1.2 Network security controls (NSCs) are configured and maintained.	X			NMI is responsible for ensuring that firewall configuration is sufficient to protect cardholder data received by its payment platform.
1.3 Network access to and from the cardholder data environment is restricted.	X			NMI is responsible for ensuring that firewall configuration is sufficient to restrict inbound traffic to and outbound traffic from CDE to only necessary services. NMI does not permit wireless technologies in the CDE.
1.4 Network connections between trusted and untrusted networks are controlled.	X	X	X	Each party is expected to limit access to and from their own network.
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.	X			NMI is responsible for ensuring that proper policies, processes, procedures and technologies are in place to protect the CDE from risk introduced by devices that connect to both untrusted and CDE networks.

Requirement 2 - Apply Secure Configurations to All System Components

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.	X	X	?	Each party is expected to maintain their own policies and procedures. NMI is responsible for ensuring passwords are correctly managed within its payment platform and all systems meet baseline security configurations.
2.2 System components are configured and managed securely.	X	?	?	Each party is required to manage their own environment as determined by their own scoping.
2.3 Wireless environments are configured and managed securely.	N/A	?	?	NMI does not permit wireless technologies in the CDE. Partner and Merchant responsibilities depend upon their network and scope.

Requirement 3 - Protect Stored Account Data

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
3.1 Processes and mechanisms for protecting stored account data are defined and understood.	X			It is assumed that NMI Partners and Merchants do not store account data. NMI is responsible for ensuring its payment platform applications and services provide suitable technical controls and secure encryption to protect CHD.
3.2 Storage of account data is kept to a minimum.	X			It is assumed that NMI Partners and Merchants do not store account data.
3.3 Sensitive authentication data (SAD) is not stored after authorization.	X			It is assumed that NMI Partners and Merchants do not capture SAD outside of the NMI solution provided.
3.4 Access to displays of full PAN and ability to copy cardholder data are restricted.	X			It is assumed that NMI Partners and Merchants do not store account data.
3.5 Primary account number (PAN) is secured wherever it is stored.	X			It is assumed that NMI Partners and Merchants do not store account data.
3.6 Cryptographic keys used to protect stored account data are secured.	X			It is assumed that NMI Partners and Merchants do not store account data.
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.	X			It is assumed that NMI Partners and Merchants do not store account data.

Requirement 4 - Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.	X	?	?	NMI is responsible for ensuring its payment platform applications and services provide suitable, cryptographic protection for card data received via its services in transit, during processing and in storage. Partner and Merchant scope will determine their responsibilities.
4.2 PAN is protected with strong cryptography during transmission.	X	?	?	Each party has a responsibility to ensure all data is securely transmitted. This includes following NMI advice for any data transfers.

Requirement 5 - Protect All Systems and Networks from Malicious Software

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.	X	?	?	Each party is responsible for their own environment. NMI is responsible for ensuring its payment platform runs appropriately configured endpoint security software including anti-virus where necessary.
5.2 Malicious software (malware) is prevented, or detected and addressed.	X	?	?	NMI has the relevant protections in place. Partner and Merchant scope will determine whether this control is relevant to them.
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.	X	?	?	NMI has the relevant protections in place. Partner and Merchant scope will determine whether this control is relevant to them.
5.4 Anti-phishing mechanisms protect users against phishing attacks.	X	?	?	NMI has the relevant protections in place. Partner and Merchant scope will determine whether this control is relevant to them.

Requirement 6 - Develop and Maintain Secure Systems and Software

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.	X			NMI is responsible for ensuring the payment applications it uses within its payment platform are secure.
6.2 Bespoke and custom software are developed securely.	X	?	?	Any custom code used in the processing of cardholder data is the responsibility of the party who created it.
6.3 Security vulnerabilities are identified and addressed.	X	?	?	Each party must manage and maintain their own environments.
6.4 Public-facing web applications are protected against attacks.	X	?	?	Each party which develops a public facing web application has a responsibility to secure, manage and maintain it.
6.5 Changes to all system components are managed securely.	X	?	?	It is assumed that NMI Partners and Merchants do not store account data. Partner and Merchant scope will determine need to implement this control.

Requirement 7 - Restrict Access to System Components and Cardholder Data to Business Need to Know

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	X	?	?	Each party should maintain its own documentation. NMI is responsible for ensuring access to cardholder data received, processed and stored in its payment platform is controlled and limited to business need to know.
7.2 Access to system components and data is appropriately defined and assigned.	X			It is assumed that NMI Partners and Merchants do not store account data.
7.3 Access to system components and data is managed via an access control system(s).	X			It is assumed that NMI Partners and Merchants do not store account data.

Requirement 8 - Identify Users and Authenticate Access to System Components

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.	X			Each party must limit access to cardholder data appropriately. NMI is responsible for authentication to its platform both by internal and external users.
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	X	?	?	NMI manages this within their environments. Partner and Merchant will depend upon scope.
8.3 Strong authentication for users and administrators is established and managed.	X	?	?	NMI manages this within their environments. Partner and Merchant will depend upon scope.
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.	X			It is assumed that NMI Partners and Merchants do not store account data.
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.	X			It is assumed that NMI Partners and Merchants do not store account data.
8.6 Use of application and system accounts and associated authentication factors is strictly managed.	X			It is assumed that NMI Partners and Merchants do not store account data.

Requirement 9 - Restrict Physical Access to Cardholder Data

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	X			NMI is responsible for ensuring access to cardholder data received, processed and stored in its payment platform is controlled and limited to business need to know.
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.	X			NMI is responsible for ensuring physical access controls are sufficient and in place to prevent unauthorized access to CDE.
9.3 Physical access for personnel and visitors is authorized and managed.	X			NMI is responsible for ensuring physical access controls are sufficient and in place to prevent unauthorized access to CDE.
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.	X			NMI is responsible for ensuring that any media containing SAD is physically secure and tracked.
9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.		X	X	Where applicable, each party must ensure this control is managed within their own environment.

Requirement 10 - Log and Monitor All Access to System Components and Cardholder Data

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.	X			It is assumed that NMI Partners and Merchants do not store account data. NMI is responsible for ensuring all access to its platform and card data stored within is monitored and tracked.
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	X			It is assumed that NMI Partners and Merchants do not store account data. NMI is responsible for ensuring all access to its platform and card data stored within is monitored, tracked and forensics capable.
10.3 Audit logs are protected from destruction and unauthorized modifications.	X			It is assumed that NMI Partners and Merchants do not store account data. NMI is responsible for ensuring all access to its platform and card data stored within is monitored, tracked and tamper-proof.
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.	X			It is assumed that NMI Partners and Merchants do not store account data. NMI is responsible for ensuring all access to its platform and card data stored within is monitored, tracked and reviewed on a cadence.

Requirement 10 - Log and Monitor All Access to System Components and Cardholder Data Continued

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
10.5 Audit log history is retained and available for analysis.	X			It is assumed that NMI Partners and Merchants do not store account data. NMI is responsible for ensuring all access to its platform and card data stored within is monitored, tracked and retained for an appropriate period of time.
10.6 Time-synchronization mechanisms support consistent time settings across all systems.	X			NMI is responsible for ensuring all platforms are time-synchronized to support proper investigation.
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.	X			NMI is responsible for ensuring that failure detection mechanisms are configured properly and that failure notices are responded to in a timeframe befitting the failure's criticality.

Requirement 11 - Test Security of Systems and Networks Regularly

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.	X	?	?	Each party is responsible for their own environment. NMI is responsible for testing and reviewing the security of its payment platform both internally and externally accessible components. NMI is responsible for ensuring that weaknesses are corrected within an appropriate period of time. Partner and Merchant will depend upon scope.
11.5 Network intrusions and unexpected file changes are detected and responded to.	X	?	?	Each party is responsible for their own environment. NMI is responsible for detecting and responded to network intrusions and unexpected file changes in an appropriate period of time. Partner and Merchant will depend upon scope.
11.6 Unauthorized changes on payment pages are detected and responded to.	X	?	?	Each party is responsible for their own environment. NMI is responsible for detecting and responded to unauthorized changes in an appropriate period of time. Partner and Merchant will depend upon scope.

Requirement 12 - Support Information Security with Organizational Policies and Programs

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.	X	X	X	Each party should have their own documented policy and maintain it. NMI is responsible for creating and maintaining information security policies and ensuring that all its employees follow them.
12.2 Acceptable use policies for end-user technologies are defined and implemented.	X			NMI is responsible for creating and maintaining acceptable use policies.
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.	X			It is assumed that NMI Partners and Merchants do not store account data.
12.4 PCI DSS compliance is managed.	X	X	X	Each party is responsible for its own compliance.
12.5 PCI DSS scope is documented and validated.	X	X	X	Each party should document and validate their own scope.
12.6 Security awareness education is an ongoing activity.	X	X	X	Each party should ensure staff are trained to handle cardholder data appropriately.

Requirement 12 - Support Information Security with Organizational Policies and Programs Continued

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
12.7 Personnel are screened to reduce risks from insider threats.	X	X	X	Each party should screen their own staff.
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.	X	X	X	Each party should manage their 3rd parties as appropriate.
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.	X	X		NMI and Partners should support Merchants where possible.
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	X	X	X	NMI and Partners are required to maintain an incident response plan that is reviewed, trained against and tested annually. TRAs should be conducted as appropriate. Incidents should be managed in a manner befitting the incident's criticality.

Appendices

	NMI	Partner	Merchant	Notes
	Party Responsible			
Control				
Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers	N/A			NMI is not a multi-tenant service provider.
Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections	N/A			NMI does not support SSL / early TLS.
Appendix A3: Designated Entities Supplemental Validation (DESV)	N/A			Not applicable to NMI.

Contact us
hello@nmi.com
www.nmi.com

Powering Every Possi
ng Every Possibility in
ossibility in Payments