

PCI DSS Shared Responsibility Matrix

Introduction

This document outlines the specific responsibilities required to maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS) when using TrendAI Vision One (formerly Trend Vision One). It is designed to comply with PCI DSS requirement 12.8.5 by clearly identifying the responsibilities of the customer, TrendAI (formerly Trend Micro), and any shared responsibilities between both parties.

TrendAI provides customers with a secure-by-design foundation through advanced security technologies and processes. Our services have been independently assessed against PCI DSS v4.0.1 requirements for the products and underlying infrastructure within our scope.

The responsibility matrix below is provided as a reference to help customers understand PCI DSS compliance roles when using TrendAI Vision One. It does not replace or override PCI DSS requirements that apply to customer-managed systems and processes. Some responsibilities belong solely to TrendAI, others to the customer, and some are shared. Customers remain accountable for meeting their overall PCI DSS compliance obligations for systems, applications, and processes under their control. Certain activities such as configurations and ongoing operations of TrendAI Vision One within the customer environment are shared responsibilities as outlined in the matrix.

Responsibility Definition

- **TrendAI responsibility**
TrendAI is responsible for implementing and maintaining PCI DSS controls within the scope of its managed services and infrastructure. These responsibilities are validated by a Qualified Security Assessor (QSA).
- **Customer responsibility**
The customer is responsible for implementing and maintaining PCI DSS controls for systems, applications, and process under their management.
- **Shared responsibility**
Both TrendAI and the customer share responsibility for certain PCI DSS requirements. TrendAI fulfills its obligation for the services within scope, while customers configure and manage their environment to maintain compliance.
- **N/A (Not Applicable)**
The requirement does not apply to the TrendAI services. This may occur when the control is outside the defined PCI DSS scope or irrelevant to the deployment model.

Shared Responsibility Matrix

PCI DSS v4.0.1 Requirements	Responsibility			
	Shared	TrendAI	Customer	N/A
Requirement 1: Install and Maintain Network Security Controls				
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood		x		
1.2 Network security controls (NSCs) are configured and maintained.		x		
1.3 Network access to and from the cardholder data environment is restricted.		x		
1.4 Network connections between trusted and untrusted networks are controlled.		x		
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.		x		
Requirement 2: Apply Secure Configurations to All System Components				
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.		x		
2.2 System components are configured and managed securely.	x			
2.3 Wireless environments are configured and managed securely.				x
Requirement 3: Protect Stored Account Data				
3.1 Processes and mechanisms for protecting stored account data are defined and understood.				x
3.2 Storage of account data is kept to a minimum.				x
3.3 Sensitive authentication data (SAD) is not stored after authorization.				x
3.4 Access to displays of full PAN and ability to copy PAN are restricted.				x
3.5 Primary account number (PAN) is secured wherever it is stored.				x
3.6 Cryptographic keys used to protect stored account data are secured.				x
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
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks				
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood.			x	
4.2 PAN is protected with strong cryptography during transmission.				x
Requirement 5: Protect All Systems and Networks from Malicious Software				
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.	x			
5.2 Malicious software (malware) is prevented or detected and addressed.		x		
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.		x		
5.4 Anti-phishing mechanisms protect users against phishing attacks.				x
Requirement 6: Develop and Maintain Secure Systems and Software				

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.		x		
6.2 Bespoke and custom software are developed securely.	x			
6.3 Security vulnerabilities are identified and addressed.		x		
6.4 Public-facing web applications are protected against attacks.		x		
6.5 Changes to all system components are managed securely.		x		
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know				
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.		x		
7.2 Access to system components and data is appropriately defined and assigned.		x		
7.3 Access to system components and data is managed via an access control system(s).		x		
Requirement 8: Identify Users and Authenticate Access to System Components				
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.		x		
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.		x		
8.3 Strong authentication for users and administrators is established and managed.	x			
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.	x			
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.	x			
8.6 Use of application and system accounts and associated authentication factors is strictly managed.	x			
Requirement 9: Restrict Physical Access to Cardholder Data				
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.				x
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.				x
9.3 Physical access for personnel and visitors is authorized and managed.				x
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.				x
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.				x
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data				
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood.	x			
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	x			
10.3 Audit logs are protected from destruction and unauthorized modifications.	x			
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.	x			
10.5 Audit log history is retained and available for analysis.	x			
10.6 Time-synchronization mechanisms support consistent time settings across all systems.		x		
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.		x		

Requirement 11: Test Security of Systems and Networks Regularly				
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.		x		
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.		x		
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.		x		
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.		x		
11.5 Network intrusions and unexpected file changes are detected and responded to.		x		
11.6 Unauthorized changes on payment pages are detected and responded to.				x
Requirement 12: Support Information Security with Organizational Policies and Programs				
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		
12.2 Acceptable use policies for end-user technologies are defined and implemented.		x		
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.		x		
12.4 PCI DSS compliance is managed.		x		
12.5 PCI DSS scope is documented and validated.		x		
12.6 Security awareness education is an ongoing activity.		x		
12.7 Personnel are screened to reduce risks from insider threats.		x		
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.		x		
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.		x		
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.		x		

Note : X - This control is relevant to the party indicated in the table