Payment Card Industry

# Data Security Standard

## Attestation of Compliance for Report on Compliance – Service Providers

**Version 4.0.1**

Publication Date: August 2024

# PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

**Entity Name: Matillion Ltd**

**Date of Report as noted in the Report on Compliance: 2025-08-22**

**Date Assessment Ended: 2025-08-13**

# Section 1: Assessment Information

## Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

### Part 1. Contact Information

| **Part 1a. Assessed Entity (ROC Section 1.1)** | |
|---|---|
| Company name: | Matillion Ltd |
| DBA (doing business as): | Matillion Ltd |
| Company mailing address: | Two New Bailey, Stanley Street, Salford, M3 5GS, Manchester, Lancashire, United Kingdom |
| Company main website: | www.matillion.com |
| Company contact name: | Mr. Graeme Park |
| Company contact title: | CISO |
| Contact phone number: | graeme.park@matillion.com |
| Contact e-mail address: | 07746725352 |

| **Part 1b. Assessor (ROC Section 1.1)** | |
|---|---|
| Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable. | |
| PCI SSC Internal Security Assessor(s) | |
| ISA name(s): | Not Applicable |
| Qualified Security Assessor | |
| Company name: | 1 Cyber Valley Limited |
| Company mailing address: | 128 City Road, London, EC1V 2NX, United Kingdom |
| Company website: | www.onecybervalley.com |
| Lead Assessor name: | Mr. Parminder Lall |
| Assessor phone number: | + 44 (0) 743 273 0425 |
| Assessor e-mail address: | parminder@onecybervalley.com |
| Assessor certificate number: | PCI QSA - 203-077 |

## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the Assessment (select all that apply):**

| | |
|---|---|
| Name of service(s) assessed: | Matillion DPC (Data Productivity Cloud) which is a Software as a Service (SaaS) platform that enables data teams to build, manage, and orchestrate data pipelines through a user-friendly, low-code interface. It helps users move, transform, and load data from various sources into cloud data warehouses. |

Type of service(s) assessed:

| **Hosting Provider:** | **Managed Services:** | **Payment Processing:** |
|---|---|---|
| ☐ Applications / software | ☐ Systems security services | ☐ POI / card present |
| ☐ Hardware | ☐ IT support | ☐ Internet / e-commerce |
| ☐ Infrastructure / Network | ☐ Physical security | ☐ MOTO / Call Center |
| ☐ Physical space (co-location) | ☐ Terminal Management System | ☐ ATM |
| ☐ Storage | ☒ Other services (specify): | ☐ Other processing (specify): |
| ☐ Web-hosting services | Using cloud native applications to host DPC which is managed by AWS cloud provider. | |
| ☐ Security services | | |
| ☐ 3-D Secure Hosting Provider | | |
| ☒ Multi-Tenant Service Provider | | |
| ☐ Other Hosting (specify): | | |
| ☐ Account Management | ☐ Fraud and Chargeback | ☐ Payment Gateway/Switch |
| ☐ Back-Office Services | ☐ Issuer Processing | ☐ Prepaid Services |
| ☐ Billing Management | ☐ Loyalty Programs | ☐ Records Management |
| ☐ Clearing and Settlement | ☐ Merchant Services | ☐ Tax/Government Payments |
| ☐ Network Provider | | |
| ☒ Others (specify): Using cloud native applications to host DPC which is managed by AWS cloud provider. | | |

***Note:*** *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

## Part 2. Executive Summary *(continued)*

### Part 2a. Scope Verification *(continued)*

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):**

| | |
|---|---|
| Name of service(s) not assessed: | Not Applicable |

Type of service(s) not assessed:

| **Hosting Provider:** | **Managed Services:** | **Payment Processing:** |
|---|---|---|
| ☐ Applications / software | ☐ Systems security services | ☐ POI / card present |
| ☐ Hardware | ☐ IT support | ☐ Internet / e-commerce |
| ☐ Infrastructure / Network | ☐ Physical security | ☐ MOTO / Call Center |
| ☐ Physical space (co-location) | ☐ Terminal Management System | ☐ ATM |
| ☐ Storage | ☐ Other services (specify): | ☐ Other processing (specify): |
| ☐ Web-hosting services | | |
| ☐ Security services | | |
| ☐ 3-D Secure Hosting Provider | | |
| ☐ Multi-Tenant Service Provider | | |
| ☐ Other Hosting (specify): | | |
| ☐ Account Management | ☐ Fraud and Chargeback | ☐ Payment Gateway/Switch |
| ☐ Back-Office Services | ☐ Issuer Processing | ☐ Prepaid Services |
| ☐ Billing Management | ☐ Loyalty Programs | ☐ Records Management |
| ☐ Clearing and Settlement | ☐ Merchant Services | ☐ Tax/Government Payments |
| ☐ Network Provider | | |
| ☐ Others (specify): | | |

| | |
|---|---|
| Provide a brief explanation why any checked services were not included in the Assessment: | Not Applicable |

### Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

| | |
|---|---|
| Describe how the business stores, processes, and/or transmits account data. | Matillion offers a data integration platform with subscription-based services. While customers may pay via credit card or cloud marketplaces (AWS/Azure), Matillion does not store or directly process cardholder data.<br>1. Cardholder Data Handling: Storage & Processing:<br>Matillion does not store or process cardholder data, is not a hosting provider and explicitly avoids hosting or processing any cardholder data directly. Matillion staff can only view the last four digits of a credit card via third party service provider Recurly admin interface which is PCI DSS Compliant. |

| | |
|---|---|
| | Cardholder data is handled exclusively by third party service provider Recurly which serves as the subscription and billing manager, Adyen is the payment gateway for card transaction processing. Both vendors are PCI DSS compliant, handling all storage, processing, and transmission of sensitive card data.<br>2. Payment Methods and Flows:<br>Matillion offers customers three primary payment methods for subscriptions: Credit Card, AWS Marketplace, and Azure Marketplace.<br>1.Credit Card Payments:<br>Customer Journey & Network Components:<br>•Matillion Website (matillion.com): Customers initiate the payment process on Matillion's website, where they select their payment method. Matillion hosts these initial "information gathering" and "checkout flow" screens.<br>•API Calls (Matillion to Recurly): When a customer chooses credit card payment, Matillion's system sends an API request to Recurly to check if a credit card is already linked to the customer's account.<br>•Redirection to Recurly-Hosted Page: If no card is on file, Matillion securely redirects the customer's browser to a Recurly-hosted page. This external page is where the customer directly enters sensitive cardholder data (credit card number, CVV, expiry date, etc.). Matillion's environment never touches this sensitive data.<br>•Recurly as Subscription and Payment Manager: Recurly serves as the primary third-party service managing subscriptions and payment collection for Matillion. It securely creates and manages the customer's payment profile, including the storage of credit card information within its PCI-compliant environment.<br>•Adyen Integration: Recurly utilizes Adyen as its payment gateway. Adyen is responsible for processing the actual transactions, including authorization and capture of funds.<br>•Payment Model: Credit card payments are primarily for recurring monthly fees (Pay-as-you-go) or for pre-purchased credits for annual contracts. Once a card is on file with Recurly, it is automatically charged when invoices are generated based on accumulated usage.<br>2.AWS and Azure Marketplace Payments:<br>•No Direct Card Handling by Matillion: Matillion explicitly states that they do not handle cardholder data for payments made through AWS or Azure Marketplaces.<br>•Account Linking and Redirection:<br>•Matillion's UI allows customers to select AWS or Azure Marketplace as their payment method.<br>•Matillion performs an API check to determine if the customer's Matillion account is linked to the respective Marketplace account. |

| | |
|---|---|
| | •If not linked, the customer is redirected to Matillion's public listing on the AWS Marketplace or Azure Marketplace for subscription.<br>•Marketplace as Payment Handler: Customers subscribe directly through the respective cloud marketplace. The marketplace (AWS or Azure) then handles all aspects of billing and payment collection using the customer's existing payment methods on file within their cloud account.<br>•Usage Reporting: Matillion aggregates customer usage data and reports this information (e.g., as a per-unit charge) to the connected AWS or Azure Marketplace.<br>•Invoice Visibility: For Marketplace customers, Matillion does not provide direct invoices. Customers view their invoices within their AWS or Azure cloud accounts, where Matillion's charges appear as a line item. Recurly still generates an "administrative invoice" for Matillion's internal revenue recognition, but this is not customer-facing.<br><br>3. Data Transmission and Networks Used<br>• Secure API Calls: Matillion's applications communicate with Recurly via API calls. These calls are essential for:<br>• Checking for existing credit card details.<br>• Sending usage events from Matillion's internal services to Recurly for billing.<br>• Controlling subscriptions for sales-led deals via an internal admin tool that leverages Recurly APIs.<br>• Redirection for Cardholder Data Input: Matillion redirects the customer's browser to Recurly-hosted pages for the secure input of credit card data. This ensures that cardholder data is transmitted directly from the customer's browser to Recurly's PCI-compliant environment over a secure connection.<br>• SSL/TLS Encryption: For all communications over public networks where Matillion's services interact with external payment components (e.g., API calls to Recurly, redirection to hosted payment pages), SSL certificates and TLS encryption are employed to ensure data confidentiality and integrity.<br>• Authentication Services: Auth0 is used by Matillion for customer authentication, and Okta is used for Recurly admin single sign-on, ensuring secure access to relevant systems. |
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | Maia's data sampling capabilities in a DPC (Data Productivity Cloud) environment are based on user control and explicit consent. It's not a mandatory feature and its use is subject to customer discretion. Customers can manage Maia's sampling feature can be handled at distinct levels:<br>•Account Level: Turn on/off Maia & Turn on/off Data sampling. The entire sampling feature can be turned off for the customer's account, resulting in a "downgraded version" of Maia without sampling. |

| | |
|---|---|
| | •User Level: Turn on/off Maia & Accept/Decline specific occurrences during Maia chat<br>Complete Deactivation: This is the most restrictive option, fully deactivating Maia and ensuring no data sampling occurs |
| Describe system components that could impact the security of account data. | Not Applicable |

## Part 2. Executive Summary *(continued)*

### Part 2c. Description of Payment Card Environment

| | |
|---|---|
| Provide a high-level description of the environment covered by this Assessment.<br>*For example:*<br>• *Connections into and out of the cardholder data environment (CDE).*<br>• *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*<br>• *System components that could impact the security of account data.* | The DPC houses Matillion's core services, including components like scheduler, Workflow, and various agents, which interact to manage data pipelines. These components handle various types of data, as indicated from the network diagrams supplied ranging from design data and secret reference data to customer data and reporting data. |
| Indicate whether the environment includes segmentation to reduce the scope of the Assessment.<br>(Refer to the "Segmentation" section of PCI DSS for guidance on segmentation) | ☐ Yes ☒ No |

### Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

| Facility Type | Total Number of Locations (How many locations of this type are in scope) | Location(s) of Facility (city, country) |
|---|---|---|
| *Example: Data centers* | *3* | *Boston, MA, USA* |
| Corporate Office | 3 | Manchester<br>Denver<br>Hyderabad |
| | | |
| | | |
| | | |
| | | |
| | | |

## Part 2. Executive Summary *(continued)*

### Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

| Name of PCI SSC validated Product or Solution | Version of Product or Solution | PCI SSC Standard to which Product or Solution Was Validated | PCI SSC Listing Reference Number | Expiry Date of Listing |
|---|---|---|---|---|
| Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| | | | | YYYY-MM-DD |
| | | | | YYYY-MM-DD |
| | | | | YYYY-MM-DD |
| | | | | YYYY-MM-DD |
| | | | | YYYY-MM-DD |

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

## Part 2. Executive Summary *(continued)*

### Part 2f. Third-Party Service Providers
*(**ROC Section 4.4**)*

For the services being validated, does the entity have relationships with one or more third-party service providers that:

| | |
|---|---|
| • Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage)) | ☒ Yes ☐ No |
| • Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers) | ☒ Yes ☐ No |
| • Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). | ☒ Yes ☐ No |

**If Yes:**

| **Name of Service Provider:** | **Description of Services Provided:** |
|---|---|
| Recurly | Payment Processing |
| AWS | Cloud Hosting Provider |
| Azure | Cloud data warehouse |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

***Note:*** *Requirement 12.8 applies to all entities in this list.*

## Part 2. Executive Summary *(continued)*

### Part 2g. Summary of Assessment (ROC Section 1.8.1)

*Indicate below all responses provided within each principal PCI DSS requirement.*

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

***Note:*** *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

*Name of Service Assessed:* Matillion DPC (Data Productivity Cloud) which is a Software as a Service (SaaS) platform that enables data teams to build, manage, and orchestrate data pipelines through a user-friendly, low-code interface. It helps users move, transform, and load data from various sources into cloud data warehouses.

| PCI DSS Requirement | Requirement Finding<br>More than one response may be selected for a given requirement. Indicate all responses that apply. | | | | Select If a Compensating Control(s) Was Used |
|---|---|---|---|---|---|
| | In Place | Not Applicable | Not Tested | Not in Place | |
| Requirement 1: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 2: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 3: | ☐ | ☒ | ☐ | ☐ | ☐ |
| Requirement 4: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 5: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 6: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 7: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 8: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 9: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 10: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 11: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Requirement 12: | ☒ | ☒ | ☐ | ☐ | ☐ |
| Appendix A1: | ☒ | ☐ | ☐ | ☐ | ☐ |
| Appendix A2: | ☐ | ☒ | ☐ | ☐ | ☐ |

**Justification for Approach**

| | |
|---|---|
| For any Not Applicable responses, identify which sub-requirements were not applicable and the reason. | 1.2.6 - There are no insecure services enabled.<br>1.3.3 - There is no wireless network in scope.<br>1.4.4 - Matillion do not store CHD in their environment.<br>2.2.5 - No insecure service running in Matillion enviornment.<br>2.3.1, 2.3.2 - There is no wireless network in scope.<br>Requirement 3 - Matillion do not store CHD in their environment.<br>4.2.1.2 - There is no wireless network in scope.<br>4.2.2 - Matillion do not use end-user messaging technology.<br>5.2.3, 5.2.3.1 - There are no system components in scope which are not at risk for malware.<br>5.3.3 - There is no removable electronic media in scope.<br>6.4.1 - This requirement is superseded by the requirement 6.4.2.<br>6.5.2 - There is no significant change in the PCI scope.<br>6.5.5 - No Live or test PAN data has been used in the environment.<br>6.5.6 - Matillion do not test off the shelf tools or third-party tools in the testing environment.<br>7.2.6 - Matillion do not store CHD in the environment.<br>8.2.2 - Matillion do not use group. shared or generic accounts.<br>8.2.3 - Matillion do not have remote access to their customer premises.<br>8.3.9 - There is no single factor authentication used in Matillion.<br>8.3.10, 8.3.10.1 - No customer user has access to Matillion environment.<br>8.6.1, 8.6.2 - No accounts have been used for interactive login.<br>9.4 - No physical media in scope.<br>9.5 - No POI devices are in scope.<br>10.7.1 - This requirement is superseded by requirement 10.7.2.<br>11.2.1, 11.2.2 - There is no wireless network in scope.<br>11.3.1, 11.3.1.2, 11.3.1.3 - There is no internal IPs in scope.<br>11.3.2.1 - There is no significant change done.<br>11.4.2 - There is no internal IPs in scope.<br>11.4.5, 11.4.6 - No segmentation is used in scope.<br>12.3.2 - There is no customised approach used.<br>12.5.3 - There is no significant change done to organizational structure.<br>Appendix A2 - No POI terminals are in scope. |
| For any Not Tested responses, identify which sub-requirements were not tested and the reason. | None |

# Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

| | |
|---|---|
| Date Assessment began:<br>***Note:*** *This is the first date that evidence was gathered, or observations were made.* | 2025-07-07 |
| Date Assessment ended:<br>***Note:*** *This is the last date that evidence was gathered, or observations were made.* | 2025-08-13 |
| Were any requirements in the ROC unable to be met due to a legal constraint? | ☐ Yes ☒ No |
| Were any testing activities performed remotely? | ☒ Yes ☐ No |

# Section 3 Validation and Attestation Details

## Part 3. PCI DSS Validation (ROC Section 1.7)

**This AOC is based on results noted in the ROC dated** *(Date of Report as noted in the ROC 2025-08-22)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)*:

| | |
|---|---|
| ☒ | **Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby (Matillion Ltd) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above. |
| ☐ | **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements.<br><br>**Target Date** for Compliance: *YYYY-MM-DD*<br><br>An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4. |
| ☐ | **Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.<br><br>This option requires additional review from the entity to which this AOC will be submitted.<br><br>*If selected, complete the following:* |

| Affected Requirement | Details of how legal constraint prevents requirement from being met |
|---|---|
| | |
| | |
| | |

## Part 3. PCI DSS Validation *(continued)*

### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**
(Select all that apply)

| | |
|---|---|
| ☒ | The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein. |
| ☒ | All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects. |
| ☒ | PCI DSS controls will be maintained at all times, as applicable to the entity's environment. |

### Part 3b. Service Provider Attestation

Graeme Park
Graeme Park (Sep 22, 2025 13:19:06 GMT+1)

| | |
|---|---|
| *Signature of Service Provider Executive Officer ↗* | Date: 2025-09-18 |
| Service Provider Executive Officer Name: Mr. Graeme Park | Title: CISO |

### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

| | |
|---|---|
| If a QSA was involved or assisted with this Assessment, indicate the role performed: | ☒ QSA performed testing procedures. |
| | ☒ QSA provided other assistance.<br>If selected, describe all role(s) performed: Auditing and Reporting |

| | |
|---|---|
| *Signature of Lead QSA ↗* | Date: 2025-09-18 |
| Lead QSA Name: Mr. Parminder Lall | |

| | |
|---|---|
| *Signature of Duly Authorized Officer of QSA Company ↗* | Date: 2025-09-18 |
| Duly Authorized Officer Name: Mr. Parminder Lall | QSA Company: 1 Cyber Valley Limited |

### Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

| | |
|---|---|
| If an ISA(s) was involved or assisted with this Assessment, indicate the role performed: | ☐ ISA(s) performed testing procedures. |
| | ☐ ISA(s) provided other assistance.<br>If selected, describe all role(s) performed: |

## Part 4. Action Plan for Non-Compliant Requirements

*Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.*

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

| PCI DSS Requirement | Description of Requirement | Compliant to PCI DSS Requirements (Select One) | | Remediation Date and Actions (If "NO" selected for any Requirement) |
|---|---|---|---|---|
| | | YES | NO | |
| 1 | Install and maintain network security controls | ☐ | ☐ | |
| 2 | Apply secure configurations to all system components | ☐ | ☐ | |
| 3 | Protect stored account data | ☐ | ☐ | |
| 4 | Protect cardholder data with strong cryptography during transmission over open, public networks | ☐ | ☐ | |
| 5 | Protect all systems and networks from malicious software | ☐ | ☐ | |
| 6 | Develop and maintain secure systems and software | ☐ | ☐ | |
| 7 | Restrict access to system components and cardholder data by business need to know | ☐ | ☐ | |
| 8 | Identify users and authenticate access to system components | ☐ | ☐ | |
| 9 | Restrict physical access to cardholder data | ☐ | ☐ | |
| 10 | Log and monitor all access to system components and cardholder data | ☐ | ☐ | |
| 11 | Test security systems and networks regularly | ☐ | ☐ | |
| 12 | Support information security with organizational policies and programs | ☐ | ☐ | |
| Appendix A1 | Additional PCI DSS Requirements for Multi-Tenant Service Providers | ☐ | ☐ | |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections | ☐ | ☐ | |

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/*

# Matillion_PCI-DSS-v4-0-1-ROC-AOC-Service-Providers_2025_Final

Final Audit Report 2025-09-23

| | |
|---|---|
| Created: | 2025-09-18 |
| By: | Parminder Lall (parminder@onecybervalley.com) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAAQS2CaXuhtrxYikG5Il9TMzLsWom4ZzZh |

## "Matillion_PCI-DSS-v4-0-1-ROC-AOC-Service-Providers_2025_Final" History

Document created by Parminder Lall (parminder@onecybervalley.com)
2025-09-18 - 2:39:18 PM GMT- IP address: 188.241.144.220

Document emailed to graeme.park@matillion.com for signature
2025-09-18 - 2:40:03 PM GMT

Email viewed by graeme.park@matillion.com
2025-09-18 - 2:58:18 PM GMT- IP address: 66.249.93.66

Signer graeme.park@matillion.com entered name at signing as Graeme Park
2025-09-22 - 12:19:04 PM GMT- IP address: 149.102.56.252

Document e-signed by Graeme Park (graeme.park@matillion.com)
Signature Date: 2025-09-22 - 12:19:06 PM GMT - Time Source: server- IP address: 149.102.56.252

Document emailed to Parminder Lall (parminder@onecybervalley.com) for signature
2025-09-22 - 12:19:07 PM GMT

Email viewed by Parminder Lall (parminder@onecybervalley.com)
2025-09-22 - 1:06:15 PM GMT- IP address: 124.217.189.37

Document e-signed by Parminder Lall (parminder@onecybervalley.com)
Signature Date: 2025-09-23 - 7:57:17 AM GMT - Time Source: server- IP address: 41.33.57.130

Agreement completed.
2025-09-23 - 7:57:17 AM GMT