Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50


# Payment Card Industry
# Data Security Standard

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

**Version 4.0.1**

Publication Date: August 2024

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50

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

**Entity Name: Datacap Systems, Inc.**

**Date of Report as noted in the Report on Compliance: August 16, 2025**

**Date Assessment Ended: August 15, 2025**


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50

# 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: | Datacap Systems, Inc. |
| DBA (doing business as): | Not Applicable |
| Company mailing address: | 100 New Britain Boulevard Chalfont, PA 18914 |
| Company main website: | https://datacapsystems.com/ |
| Company contact name: | Anthony Sanchez |
| Company contact title: | Director of Engineering |
| Contact phone number: | 215-997-8989 |
| Contact e-mail address: | anthony.sanchez@dcap.com |

| **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: | Moss Adams LLP |
| Company mailing address: | 999 Third Avenue Suite 2800 Seattle, WA 98104 |
| Company website: | https://mossadams.com |
| Lead Assessor name: | Jonathan Smith |
| Assessor phone number: | (801) 907-4332 |
| Assessor e-mail address: | jonathan.smith@mossadams.com |
| Assessor certificate number: | QSA, 203-131 |


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



## 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: | NETePay Hosted Platform | |
|---|---|---|
| Type of service(s) assessed: | | |
| **Hosting Provider:**<br>☐ Applications / software<br>☐ Hardware<br>☐ Infrastructure / Network<br>☐ Physical space (co-location)<br>☐ Storage<br>☐ Web-hosting services<br>☐ Security services<br>☐ 3-D Secure Hosting Provider<br>☐ Multi-Tenant Service Provider<br>☐ Other Hosting (specify): | **Managed Services:**<br>☐ Systems security services<br>☐ IT support<br>☐ Physical security<br>☐ Terminal Management System<br>☐ Other services (specify): | **Payment Processing:**<br>☒ POI / card present<br>☒ Internet / e-commerce<br>☐ MOTO / Call Center<br>☐ ATM<br>☐ Other processing (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): | | |

***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.*


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



## 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: | Prepaid gift program through the NETePay Hosted platform |

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): Prepaid gift program through the NETePay Hosted platform

| | |
|---|---|
| Provide a brief explanation why any checked services were not included in the Assessment: | Datacap has elected to exclude this service from the scope of this assessment. |

### 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. | Datacap hosts a payment gateway that sends credit card transactions to payment processors in the US and Canada.<br>Transmit:<br>The NETePay Hosted gateway receives and transmits card data to payment processors or other validated third parties. The card data is transported using TLS 1.2 and encrypted via AES-256.<br>Process:<br>The NETePay Hosted gateway processes card data at a single point in the payment flow. A secure application |


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



| | |
|---|---|
| | has the capability to decrypt E2E encrypted card data and run bin checks against that data for processing rules. The card data is then sent to a payment processor for authorization.<br>Store:<br>The NETePay Hosted gateway stores card data in SQL and COSMOS databases in Microsoft Azure. Credit card data is file-level encrypted using AES-256 and Blowfish (512 bit). |
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | Not Applicable |
| Describe system components that could impact the security of account data. | Critical components of the cardholder data environment included:<br>Azure Network Security Controls – Externally facing firewalls to control incoming traffic and provide network segmentation.<br>Azure Network Load Balancers – Used to manage traffic loads.<br>Windows and Linux Servers – Utilized to host the application, processing servers, etc.<br>Workstations – Used by end users to manage / administer the CDE.<br>Azure Cloud Console – used to manage cloud services.<br>MFA – used to provide multi-factor authentication to in scope services.<br>Centralized Logging – Used to aggregate, store, and analyze security events.<br>Security Tools – Used to monitor the environment for intrusion attempts, unauthorized file changes, etc. |


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



## 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 cardholder data environment was hosted and supported by Azure networks and services. Connections into and out of the Azure environments included TLS 1.2 connections for cardholder data transmission, as well as HTTPS connections for management. Critical components of the cardholder data environment included:<br>Azure Network Security Controls – Externally facing firewalls to control incoming traffic and provide network segmentation.<br>Azure Network Load Balancers – Used to manage traffic loads.<br>Windows and Linux Servers – Utilized to host the application, processing servers, etc.<br>Workstations – Used by end users to manage / administer the CDE.<br>Azure Cloud Console – used to manage cloud services.<br>MFA – used to provide multi-factor authentication to in scope services.<br>Centralized Logging – Used to aggregate, store, and analyze security events.<br>Security Tools – Used to monitor the environment for intrusion attempts, unauthorized file changes, etc. |
| 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* |
| Azure Hosted Region | 4 | Azure East US 2<br>Azure West US 2<br>Azure Central US<br>Azure South Central US |
| | | |


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



| | | |
|---|---|---|
| | | |
| | | |
| | | |
| | | |


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

## 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 |
|---|---|---|---|---|
| NETePay 5 | 5.08 | Secure Software Standard v1.1 | 22-45.00037.001 | 2025-12-16 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

* 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.


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



## 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: |
|---|---|
| Microsoft Azure | Cloud Hosting Provider, Identity Management |
| Bluefin Payment Solutions | P2PE Services |
| Spreedly | Tokenization/Account Updater |
| TrendMicro | IDS/IPS, File Integrity Monitoring |
| Github | Code Repository |
| | |
| | |
| | |
| | |
| | |

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


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

## 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:* NETePay Hosted Platform

| 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**


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



| | |
|---|---|
| For any Not Applicable responses, identify which sub-requirements were not applicable and the reason. | 1.3.3, 2.3.1, 2.3.2, 4.2.1.2; There were no wireless networks in scope.<br>2.2.5; N/A – No insecure services running on in-scope system components<br>3.3.1.1; N/A - Full track data was not received or stored.<br>3.3.3; N/A – Datacap is not an issuer and does not support issuing services.<br>3.5.1.2, 3.5.1.3; Disk–level encryption was not in use.<br>3.7.9; N/A – Datacap did not share cryptographic keys.<br>4.2.2; N/A – Datacap did not utilize end-user messaging technologies to send transmit / receive PAN.<br>5.2.3, 5.2.3.1; An anti-malware solution was deployed on all in-scope system components where a full anti-malware solution was able to be deployed.<br>5.3.2.1; Datacap relied on continuous behavioral analysis (not scanning).<br>6.4.1; This requirement is superseded by 6.4.2<br>6.4.3, 11.6.1; Datacap did not host payment pages.<br>8.2.3; Datacap did not have remote access to any customer premises.<br>8.2.7; No third parties had access to in-scope systems.<br>8.3.9; Passwords were not used as the only authentication mechanism as Microsoft Entra ID had MFA enabled and required.<br>8.3.10; This requirement has been superseded by 8.3.10.1.<br>8.3.10.1; Non-consumer customer user accounts did not exist on in-scope systems.<br>9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7; Datacap did not capture or store any physical media with cardholder data.<br>9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3, Appendix A2; Datacap did not manage POI devices to interact with account data.<br>10.4.2, 10.4.2.1; Logs of all system components were reviewed daily.<br>10.7.1; This requirement is superseded by 10.7.2.<br>11.3.2.1; No externally facing significant changes occurred during the testing period.<br>11.4.7, Appendix A1; Datacap is not a multi-tenant service provider.<br>12.3.2; Datacap did not utilize the customized approach to meet any applicable requirement.<br>12.5.3; A significant organizational structure change did not occur within the last year.<br>Appendix A3; Datacap was not required to complete this appendix. |
| For any Not Tested responses, identify which sub-requirements were not tested and the reason. | Not Applicable |


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



# 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.* | 2025-05-07 |
| Date Assessment ended:<br>***Note:*** *This is the last date that evidence was gathered, or observations were made.* | 2025-08-15 |
| 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 |


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



# 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 2025-08-16)*.

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 Datacap Systems, Inc. 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 |
|---|---|
| | |
| | |
| | |


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



## 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

DocuSigned by:
Anthony Sanchez
03D9B63D15324EB...

| | |
|---|---|
| *Signature of Service Provider Executive Officer ↑* | Date: 8/18/2025 |
| Service Provider Executive Officer Name: Anthony Sanchez | Title: Director of Engineering |

### 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: |

DocuSigned by:
Jonathan Smith
2D38ED022A9D4EB...

| | |
|---|---|
| *Signature of Lead QSA ↑* | Date: 8/18/2025 |
| Lead QSA Name: Jonathan Smith | |

Signed by:
Casey Wassom
33E9324C25EA4B7...

| | |
|---|---|
| *Signature of Duly Authorized Officer of QSA Company ↑* | Date: 8/18/2025 |
| Duly Authorized Officer Name: Casey Wassom | QSA Company: Moss Adams LLP |

### 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: |


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*

Docusign Envelope ID: 1B29264E-2108-43F1-ACC1-031BB75EEF50



## 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/*


*© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.*