



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 2

Publication Date: August 2023



PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Systems East, Inc.

Assessment End Date: April 24th, 2024

Date of Report as noted in the Report on Compliance: April 29th, 2024



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: | Systems East, Inc |
| DBA (doing business as): | |
| Company mailing address: | 50 Clinton Avenue Cortland, NY 13045 |
| Company main website: | https://www.systemseast.com |
| Company contact name: | Peter Rogati |
| Company contact title: | Director of Operations |
| Contact phone number: | +1 (607)753-6156 |
| Contact e-mail address: | peter@systemseast.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): | N/A |
| Qualified Security Assessor | |
| Company name: | Securisea |
| Company mailing address: | 2501 Chatham Rd Suite 4573 Springfield, IL 62704 |
| Company website: | https://www.securisea.com/ |
| Lead Assessor name: | Thomas Porter |
| Assessor phone number: | +1 (877) 563-4230 x410 |



| | |
|------------------------------|-----------------------|
| Assessor e-mail address: | tporter@securisea.com |
| Assessor certificate number: | 206-677 |

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: | Xpress-pay.com | |
| Type of service(s) assessed: | | |
| Hosting Provider: <input checked="" type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify): | Managed Services: <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify): | Payment Processing: <input type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input checked="" type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify): |
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Fraud and Chargeback | <input checked="" type="checkbox"/> Payment Gateway/Switch |
| <input type="checkbox"/> Back-Office Services | <input type="checkbox"/> Issuer Processing | <input type="checkbox"/> Prepaid Services |
| <input type="checkbox"/> Billing Management | <input type="checkbox"/> Loyalty Programs | <input type="checkbox"/> Records Management |
| <input type="checkbox"/> Clearing and Settlement | <input type="checkbox"/> Merchant Services | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Network Provider | | |
| <input type="checkbox"/> 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.



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:

Electronic payment services as selected below.

Type of service(s) not assessed:

Hosting Provider:

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web-hosting services
- Security services
- 3-D Secure Hosting Provider
- Multi-Tenant Service Provider
- Other Hosting (specify):

Managed Services:

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

Payment Processing:

- POI / card present
- Internet / e-commerce
- MOTO / Call Center
- ATM
- 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):

Provide a brief explanation why any checked services were not included in the Assessment:

The above checked services do not involve any transmission, processing, or storage of CHD.

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.

Systems East stores, processes, and transmits cardholder data (CHD) entirely within its outsourced cloud environment hosted by Flexential. Systems East's web and application servers running its ecommerce application Xpress-pay.com receive transactions (including CHD) via a TLS-encrypted browser connections and encrypts and stores the CHD within a SQL Server database for subscription or reoccurring payments. Systems East transmits CHD for authorization to payment processors or acquirers via the processors' PCI-compliant payment APIs.



| | |
|--|---|
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | Systems East does not directly or otherwise impact the security of its clients' CDEs other than sharing of CHD which is covered in the scope of the assessment. |
| Describe system components that could impact the security of account data. | The relevant system components are limited to the inscope payment applications and databases within the Flexential-supported infrastructure. |



Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment.

For example:

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
- *System components that could impact the security of account data.*

Systems East CDE includes its dedicated PCI operational systems held within the Flexential-supported infrastructure, which houses all in scope servers, software and storage, and also Fexentail's dedicated Azure identity management that houses all user identity and access permissions information.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment.

(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) |
|-------------------------------|---|--|
| <i>Example: Data centers</i> | 3 | <i>Boston, MA, USA</i> |
| Corporate Office | 1 | Cortland, NY |
| Flexential Data Center | 1 | Allentown, PA |
| Systems East Corporate Office | 1 | Cortland, NY |
| | | |
| | | |
| | | |



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 |
|---|--------------------------------|---|----------------------------------|------------------------|
| | | | | YYYY-MM-DD |
| | | | | 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, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.



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:

| | |
|--|---|
| <ul style="list-style-type: none"> • 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)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <ul style="list-style-type: none"> • 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) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <ul style="list-style-type: none"> • Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

If Yes:

| Name of Service Provider: | Description of Services Provided: |
|----------------------------------|--|
| Flexential, LLC | IaaS |
| Authorize.net | Payment processor |
| Converge (Elavon) | Payment processor |
| TSYS | Payment processor |
| USAePay | Payment processor |
| WorldPay | Payment processor |
| Forte Payment Systems | Payment processor |
| | |
| | |
| | |

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:

| PCI DSS Requirement | Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply. | | | | Select If Below Method(s) Was Used | |
|---------------------|---|-------------------------------------|--------------------------|--------------------------|------------------------------------|-------------------------------------|
| | In Place | Not Applicable | Not Tested | Not in Place | Customized Approach | Compensating Controls |
| Requirement 1: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 2: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 3: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 4: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 5: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 6: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Requirement 7: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 8: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 9: | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 10: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 11: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 12: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Appendix A1: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Appendix A2: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Justification for Approach



For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

1.2.6 - Systems East does not employ any insecure services, protocols, or services.

1.3.3 - N/A - No wireless networks are in scope or connected to the CDE

2.3.1 - N/A - Observed that the entire CDE exists within Flexential's infrastructure who's AOC states no connected wireless environments exist.

2.3.2 - N/A - Observed that the entire CDE exists within Flexential's infrastructure and thus no connected wireless environments exist.

3.3.1.1 - N/A - QSA reviewed proprietary AI systems & proprietary chat systems and confirmed Systems East does not receive any Track Data.

3.3.1.2 - N/A - QSA reviewed proprietary AI systems & proprietary chat systems and confirmed Systems East does not receive any CVC data.

3.3.1.3 - N/A - QSA reviewed proprietary AI systems & proprietary chat systems and confirmed Systems East does not receive any PIN Data.

3.3.2 - N/A - QSA reviewed proprietary AI systems & proprietary chat systems and confirmed Systems East does not receive any SAD data.

3.3.3 - N/A - Systems East is not an issuer and does not support issuing operations.

3.4.2 - N/A – Best Practice until March 31, 2025.

3.5.1.1 - N/A – Best Practice until March 31, 2025.

3.6.1.1 - N/A – Best Practice until March 31, 2025.

3.6.1.3 - N/A - Systems East does use cleartext cryptographic keys

3.7.6 - N/A - Systems East does use cleartext cryptographic key

3.7.9 - N/A - Systems East does not share keys

4.2.1.1 - N/A – Best Practice until March 31, 2025

4.2.1.2 - N/A -- Observed that the entire CDE exists within Flexential's infrastructure and thus no connected wireless environments exist

4.2.2 - N/A - PAN is never sent over end user technologies

5.2.3 - N/A - Although they have systems that are not commonly affected, they have AV installed

5.2.3.1 - N/A – Best Practice until March 31, 2025.

5.3.1 - N/A – Best Practice until March 31, 2025.

5.3.2.1 - N/A – Best Practice until March 31, 2025.

5.3.3 - N/A – Best Practice until March 31, 2025.

5.4.1 - N/A – Best Practice until March 31, 2025.

6.3.2 - N/A – Best Practice until March 31, 2025.

6.4.2 - N/A – Best Practice until March 31, 2025.

6.4.3 - N/A – Best Practice until March 31, 2025.

7.2.4 - N/A – Best Practice until March 31, 2025.

7.2.5 - N/A – Best Practice until March 31, 2025.

7.2.5.1 - N/A – Best Practice until March 31, 2025.



| | |
|--|--|
| | <p>8.2.3 - N/A - No remote access into customers systems.</p> <p>8.2.7 - N/A – Systems East does not allow any 3rd party access to its CDE.</p> <p>8.3.6 - N/A - Best Practice until March 31, 2025</p> <p>8.3.10 - N/A - Best Practice until March 31, 2025</p> <p>8.3.10.1 - N/A - Best Practice until March 31, 2025</p> <p>8.4.2 - N/A - Best Practice until March 31, 2025</p> <p>8.5.1 - N/A - Best Practice until March 31, 2025</p> <p>8.6.1 - N/A - Best Practice until March 31, 2025</p> <p>8.6.2 - N/A - Best Practice until March 31, 2025</p> <p>8.6.3 - N/A - Best Practice until March 31, 2025</p> <p>9.5.1 - N/A - Systems East does not use POI devices</p> <p>9.5.1.1 - N/A - Systems East does not use POI device</p> <p>9.5.1.2 - N/A - Systems East does not use POI devices</p> <p>9.5.1.2.1 - N/A - Systems East does not use POI devices</p> <p>9.5.1.3 - N/A - Systems East does not use POI devices</p> <p>10.4.1.1 - N/A - Best Practice until March 31, 2025</p> <p>10.4.2.1 - N/A - Best Practice until March 31, 2025</p> <p>10.7.2 - N/A - Best Practice until March 31, 2025</p> <p>11.3.1.1 - N/A - Best Practice until March 31, 2025</p> <p>11.3.1.2 - N/A - Best Practice until March 31, 2025</p> <p>11.3.1.3 - N/A - There was no significant changes in the last 12 months</p> <p>11.3.2.1 - N/A - There was no significant changes in the last 12 months</p> <p>11.4.7 - N/A - Best Practice until March 31, 2025</p> <p>11.5.1.1 - N/A - Best Practice until March 31, 2025</p> <p>11.6.1 - N/A - Best Practice until March 31, 2025</p> <p>12.3.1 - N/A - Best Practice until March 31, 2025</p> <p>12.3.3 - N/A - Best Practice until March 31, 2025</p> <p>12.3.4 - N/A - Best Practice until March 31, 2025</p> <p>12.5.2.1 - N/A - Best Practice until March 31, 2025</p> <p>12.5.3 - N/A - Best Practice until March 31, 2025</p> <p>12.6.2 - N/A - Best Practice until March 31, 2025</p> <p>12.6.3.1 - N/A - Best Practice until March 31, 2025</p> <p>12.6.3.2 - N/A - Best Practice until March 31, 2025</p> <p>12.10.4.1 - N/A - Best Practice until March 31, 2025</p> <p>12.10.7 - N/A - Best Practice until March 31, 2025</p> <p>A1 - Systems East is not a multi-tenant service provider.</p> <p>A2 - Systems East does not use any early SSL/TLS</p> |
| <p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p> | <p>N/A</p> |



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

| | | |
|---|---|---|
| Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i> | | 2024-03-26 |
| Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i> | | 2024-04-23 |
| Were any requirements in the ROC unable to be met due to a legal constraint? | | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed: | | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| • Examine documentation | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| • Interview personnel | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| • Examine/observe live data | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| • Observe process being performed | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| • Observe physical environment | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| • Interactive testing | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| • Other: | <input type="checkbox"/> Yes | <input type="checkbox"/> 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 2024-04-29)*.

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 Systems East, 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.

Target Date for Compliance: YYYY-MM-DD

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.

This option requires additional review from the entity to which this AOC will be submitted.

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)

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | The ROC was completed according to <i>PCI DSS</i> , Version 4.0 and was completed according to the instructions therein. |
| <input checked="" type="checkbox"/> | All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects. |
| <input checked="" type="checkbox"/> | PCI DSS controls will be maintained at all times, as applicable to the entity's environment. |

Part 3b. Service Provider Attestation

| | |
|--|-------------------------------|
| DocuSigned by: <i>Peter T Rogati II</i> | |
| <small>2E11B814C56C4C0...</small> | |
| Signature of Service Provider Executive Officer ↑ | Date: 4/29/2024 |
| Service Provider Executive Officer Name: Peter T Rogati II | Title: Director of Operations |

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

| | |
|--|---|
| If a QSA was involved or assisted with this Assessment, indicate the role performed: | <input checked="" type="checkbox"/> QSA performed testing procedures. |
| | <input type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed: |
| DocuSigned by: <i>Thomas Porter</i> | |
| <small>131D97A8AC9B491...</small> | |
| Signature of Lead QSA ↑ | Date: 2024-04-29 |
| Lead QSA Name: Thomas Porter | |

| | |
|---|------------------------------|
| DocuSigned by: Josh Daymont | |
| <small>CF838494882345C...</small> | |
| Signature of Duly Authorized Officer of QSA Company ↑ | Date: 4/29/2024 |
| Duly Authorized Officer Name: Josh Daymont | QSA Company: Securisea, Inc. |

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

| | |
|--|--|
| If an ISA(s) was involved or assisted with this Assessment, indicate the role performed: | <input type="checkbox"/> ISA(s) performed testing procedures. |
| | <input type="checkbox"/> ISA(s) provided other assistance. 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 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 2 | Apply secure configurations to all system components | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 3 | Protect stored account data | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 4 | Protect cardholder data with strong cryptography during transmission over open, public networks | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 5 | Protect all systems and networks from malicious software | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 6 | Develop and maintain secure systems and software | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 7 | Restrict access to system components and cardholder data by business need to know | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 8 | Identify users and authenticate access to system components | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 9 | Restrict physical access to cardholder data | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 10 | Log and monitor all access to system components and cardholder data | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 11 | Test security systems and networks regularly | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12 | Support information security with organizational policies and programs | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| Appendix A1 | Additional PCI DSS Requirements for Multi-Tenant Service Providers | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |

