**security**METRICS®

PCi Security
Standards Council ®

# Payment Card Industry (PCI)

# Data Security Standard

# Attestation of Compliance for Self Assessments - Service Providers

**Version 3.2.1**

April 2024

# Attestation of Compliance, SAQ D-SP 3.2.1

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the merchant's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

### Part 1. and Qualified Security Assessor Information

#### Part 1a. Organization Information

| | | | |
|---|---|---|---|
| Company Name: | Suran Systems, Inc. | DBA (doing business as): | |
| Contact Name: | Alex Clay | Title: | CEO |
| Telephone: | 8592515236 | E-mail: | alex@suran.com |
| Business Address: | 695 Craigs Creek Rd. | City: | Versailles |
| State/Province: | KY | Country: | United States | Zip: 40383 |
| URL: | https://www.suran.com | | |

#### Part 1b. Qualified Security Assessor Company Information (Not applicable: self-attested)

| | | | |
|---|---|---|---|
| Company Name: | | | |
| Lead QSA Contact Name: | | Title: | |
| Telephone: | | E-mail: | |
| Business Address: | | City: | |
| State/Province: | | Country: | Zip: |
| URL: | | | |

securityMETRICS®

## Part 2. Executive Summary

### Part 2a. Scope Verification

### Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

| Name of service(s) assessed: | |
|---|---|

Type of service(s) assessed:

| **Hosting Provider:** | **Managed Services (specify):** | **Payment Processing:** |
|---|---|---|
| ☑ Applications / Software | ☐ Systems security services | ☐ POS / 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 | | |
| ☐ Security services | | |
| ☐ 3-D Secure Hosting Provider | | |
| ☑ Shared Hosting 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): | Application integration with payment processor | |

**Note:** These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete \"Others\". If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

### Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

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

Type of service(s) not assessed:

| Hosting Provider: | Managed Services (specify): | Payment Processing: |
|---|---|---|
| ☐ Applications / Software | ☐ Systems security services | ☐ POS / 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 | | |
| ☐ Security services | | |
| ☐ 3-D Secure Hosting Provider | | |
| ☐ Shared Hosting 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: | | |

## Part 2b. Description of Payment Card Business

| | |
|---|---|
| Describe how and in what capacity your business stores, processes, and/or transmits cardholder aoc_data. | Suran develops, sells, and supports software solutions the non-profit and faith-based sector. Our clients use our applications to submit charitable donations and payments for event (child camp, fundraiers, etc.) |
| How and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data? | None. All management of giver data is performed by our customers and uses tokens. |

## Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

| Type of facility | Number of facilities of this type | Location(s) of facility (city, country) |
|---|---|---|
| Cloud hosting provider (Linode) | 1 | Atlanta, GA |

securityMETRICS®

## Part 2d. Payment Application

Does the organization use one or more Payment Applications?  ☐ Yes  ☑ No

## Part 2e. Description of Environment

| Provide a **_high-level_** description of the environment covered by this assessment.<br>For example:<br><br>• Connections into and out of the cardholder data environment (CDE)<br>• Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable | Our CDE is a secure, single-purpose application on a dedicated, firewalled virtual machine that translates PAN to our payment processor. No PAN is retained or stored. Tokens are used to initiate payments. Access to the CDE is tightly restricted to senior staff. |
|---|---|

| Does your business use network segmentation to affect the scope of your PCI DSS environment?<br>*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)* | ☑ Yes  ☐ No |
|---|---|

## Part 2f. Third-Party Service Providers

| Does your company use a Qualified Integrator & Reseller (QIR)? | ☐ Yes  ☑ No |
|---|---|
| Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)? | ☑ Yes  ☐ No |

| Name of service provider: | Description of services provided: |
|---|---|
| Paragon Payment Solutions | Payment Gateway |

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

## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- Full - The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the SAQ.
- Partial - One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the SAQ.
- None All sub-requirements of that requirment were marked as "Not Tested" and/or "Not Applicable" in the SAQ.

For all requirements identified as either "Partial" or "None", provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the SAQ.
- Reason why sub-requirement(s) were not tested or not applicable

*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:** | |
|---|---|

| Details of Requirements Assessed | | | | |
|---|---|---|---|---|
| **PCI DSS Requirement** | **Full** | **Partial** | **None** | **Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.) |
| 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 A: | ☐ | ☐ | ☐ | |
|---|---|---|---|---|

# Section 2: Self-Assessment Questionnaire D-SP

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying Self-Assessment Questionnaire (SAQ).

| | |
|---|---|
| The assessment documented in this attestation and in the SAQ was completed on: | 2024-03-22 |
| Have compensating controls been used to meet any requirement in the SAQ? | ☐ Yes  ☑ No |
| Were any requirements in the SAQ identified as being not applicable (N/A)? | ☐ Yes  ☑ No |
| Were any requirements in the SAQ identified as being not tested? | ☐ Yes  ☑ No |
| Were any requirements in the SAQ unable to be met due to legal constraint? | ☐ Yes  ☑ No |

# Section 3: Validation and Attestation Details

## Part 3. PCI DSS Validation

**This AOC is based on results noted in the SAQ D-SP dated (2024-03-22).**

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

| | |
|---|---|
| ☑ | **Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Suran Systems, Inc.* has demonstrated full compliance with PCI DSS. |
| ☐ | **Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions answered affirmatively, resulting in an overall **NON-COMPLIANT** rating; thereby *Suran Systems, Inc.* has not demonstrated full compliance with PCI DSS.<br>**Target Date** for Compliance:<br>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.* |
| ☐ | **Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. |

## Part 3a. Acknowledgement of Status

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

| | |
|---|---|
| ☑ | PCI DSS Self-Assesment Questionnaire D-SP, Version 3.2.1, was completed according to the instructions therein. |
| ☑ | All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects. |
| ☑ | I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times. |
| ☑ | If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply. |
| ☑ | No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during this assessment. |

## Part 3b. Attestation

ELECTRONICALLY ATTESTED

| | |
|---|---|
| *Signature of Executive Officer ^* | *Date:* 2024-03-22 |
| *Executive Officer Name:* Alex Clay | *Title:* CEO |

**security**METRICS®

| **Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)** | |
| --- | --- |
| If a QSA was involved or assisted with this assessment, describe the role performed: | |

N/A: Self-Attested only

| *Signature of Duly Authorized Officer of QSA Company ^* | *Date:* |
| --- | --- |
| *Duly Authorized Officer Name:* | *QSA Company:* |

| **Part 3d. Internal Security Assessor (ISA) Acknowledgement (if applicable)** | |
| --- | --- |
| If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed: | |