Payment Card Industry
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D for Service Providers

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: December 2024

Section 1: Assessment Information

Instructions for Submission

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

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information	
Part 1a. Assessed Entity	
Company name:	Atlas Systems, Inc.
DBA (doing business as):	Aeon
Company mailing address:	5712 Cleveland St #200 Virginia Beach, VA 23462
Company main website:	https://www.atlas-sys.com/
Company contact name:	Kathy Poston
Company contact title:	Director of ITS
Contact phone number:	757-276-7660
Contact e-mail address:	kposton@atlas-sys.com
Part 1b. Assessor	
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:	Pointe Solutions Inc.
Company mailing address:	PO Box 41 Exton PA 19341
Company website:	www.pointesolutionsinc.com
Lead Assessor Name:	Hugh Burke
Assessor phone number:	610-524-1230
Assessor e-mail address:	hugh@pointesolutionsinc.com
Assessor certificate number:	PCI QSA – Certificate # 200-791

Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed:	Aeon

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		
☐ 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):		

***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 PCI DSS 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:	

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	The Aeon web server software hosts customer websites that redirect to the payment processors.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Atlas Systems provides managed services for subscribed customers of the Aeon software product.
Describe system components that could impact the security of account data.	E-Commerce Aeon redirects e-Commerce transactions to a PCI DSS certified third party prior to entering cardholder data (CHD) to purchase goods from their website.

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.*	Aeon's e-commerce network uses web servers to transmit customer's transaction information, not cardholder data (CHD), within a shopping cart to a third-party hosted and managed payment page to process card-not-present transactions. In this environment, the Aeon web servers contain the mechanism that redirects customers from their website to a third-party service provider, contracted by the customer, for payment processing using a redirect
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities—for example, corporate offices, data centers, call centers, and mail rooms—in scope for the PCI DSS 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*
Atlas Corporate Headquarters	1	Virginia Beach, Virginia
Microsoft Azure	1	USA

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions

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)
Not Applicable				

♦ 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

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 scope of the entity's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, 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 service(s) provided:**
Microsoft Azure	Hosting Provider / Managed Services

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

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: Aeon

PCI DSS Requirement	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	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.	3.1.1 through 3.7.9, 4.1.1 through 4.2.2, 6.5.5, 6.5.6, 7.2.6, 8.2.1, 9.4.1 through 9.4.7, 10.1.1 through 10.7.3 Aeon does not transmit, process or store CHD. 2.3.1, 2.3.2 No wireless networks are connected to the Aeon CDE. 5.3.3 System components with removable media are segregated from the CHD environment. 8.3.10 This requirement was superseded by Requirement 8.3.10.1. 9.5.1 through 9.5.1.3, A2.1.1 through A2.1.3 Aeon does not process transactions using point-of-interaction (POI) devices. 11.4.7, A1.1.1 through A1.2.3 Aeon is not a multi-tenant service provider.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2026/04/30
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated (Self-assessment completion date *2026-04-30*).

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

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

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

Based on the results documented in the SAQ D 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 SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Atlas Systems, Inc.* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ 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 the PCI DSS requirements included in this SAQ. **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 PCI DSS SAQ 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 1) In Place, 2) In Place with CCW, or 3) 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 included in this SAQ 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 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	*PCI DSS Self-Assessment Questionnaire D, Version 4.0.1,* was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's 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

M. Jason Glover

M. Jason Glover (May 1, 2026 08:26:01 EDT)

Signature of Service Provider Executive Officer ↑	*Date:* May 1, 2026
Service Provider Executive Officer Name: **Jason Glover**	*Title:* **President**

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. If selected, describe all role(s) performed:

Hugh Burke

Signature of Lead QSA ↑	*Date:* Apr 30, 2026
Lead QSA Name: **Hugh Burke**	

Hugh Burke

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* Apr 30, 2026
Duly Authorized Officer Name: **Hugh Burke**	*QSA Company:* **Pointe Solutions, 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:	☐ ISA(s) performed testing procedures.
	☐ 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 a Non-Compliant status 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 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 its program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/.*

2026 Atlas PCI-DSS-v4-0-1-AOC-for-SAQ-D-Service-Provider-r1 FINAL

Final Audit Report 2026-05-01

Created:	2026-04-30
By:	Hugh Burke (hugh@pointesolutionsinc.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAFwbEhgv8snj50Csvth0MzpKwRcwd-f-O

"2026 Atlas PCI-DSS-v4-0-1-AOC-for-SAQ-D-Service-Provider-r1 FINAL" History

Document created by Hugh Burke (hugh@pointesolutionsinc.com)
2026-04-30 - 4:49:04 PM GMT

Document e-signed by Hugh Burke (hugh@pointesolutionsinc.com)
Signature Date: 2026-04-30 - 4:50:53 PM GMT - Time Source: server

Document emailed to Jason Glover (jglover@atlas-sys.com) for signature
2026-04-30 - 4:50:57 PM GMT

Email viewed by Jason Glover (jglover@atlas-sys.com)
2026-05-01 - 12:19:11 PM GMT

Signer Jason Glover (jglover@atlas-sys.com) entered name at signing as M. Jason Glover
2026-05-01 - 12:25:59 PM GMT

Document e-signed by M. Jason Glover (jglover@atlas-sys.com)
Signature Date: 2026-05-01 - 12:26:01 PM GMT - Time Source: server

Agreement completed.
2026-05-01 - 12:26:01 PM GMT