



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

Section 1: Assessment Information

Instructions for Submission

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

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	Elasticsearch, Inc.	DBA (doing business as):	Elasticsearch		
Contact Name:	Abby Zumstein	Title:	Sr. Manager, Customer Trust and Assurance		
Telephone:	770-401-5904	E-mail:	Abby.Zumstein@elastic.co		
Business Address:	88 Kearny St., Floor 19	City:	San Francisco		
State/Province:	CA	Country:	USA	Zipcode:	94108
URL:	https://elastic.co				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Kevin Wieting	Title:	Principal		
Telephone:	877-224-8077	E-mail:	coalfiresubmission@coalfire.com		
Business Address:	8480 E. Orchard Rd., Suite 5800	City:	Greenwood Village		
State/Province:	CO	Country:	USA	Zip:	80111
URL:	https://www.coalfire.com				

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: Elasticsearch Service on the Elastic Cloud (ESS) and Elasticsearch Service Private (ESSP)

Type of service(s) assessed:

Hosting Provider:

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

Managed Services (specify):

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

Payment Processing:

- POS / 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):

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.

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 (check all that apply):

Name of service(s) not assessed:		Not Applicable
Type of service(s) not assessed:		
Hosting Provider: <input 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 <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services (specify): <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"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input 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 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):		
Provide a brief explanation why any checked services were not included in the assessment:		Not Applicable

Part 2b. Description of Payment Card Business

<p>Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.</p>	<p>Elasticsearch, Inc. (Elastic) operates as a Level 1 Managed Service Provider, specializing in offering search capabilities and a variety of products and solutions, notably including the Elastic Stack, formerly recognized as the ELK Stack. The company's primary focus revolves around developing and supporting real-time search and analytics solutions, catering to a diverse clientele across industries, including enterprises, government organizations, and startups.</p> <p>Elastic does not possess an Acquiring Bank to validate or endorse its position. Consequently, every customer of Elastic Cloud is required to assume both risks and responsibilities when employing the Elastic Cloud-hosted Software as a Service (SaaS) solution to meet their PCI-related business requirements. Elastic itself does not engage in handling, storing, or processing in-scope PCI Data as an intrinsic part of its business model; however, its customers might manage cardholder data. The security of such data is deemed a shared responsibility, and Elastic may or may not gain logical access to its customer's data.</p> <p>By providing versatile and comprehensive solutions, Elastic serves a broad spectrum of applications such as search, logging, security, and analytics, enabling their customers to efficiently manage and analyze large volumes of data.</p>
<p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p>	<p>Elastic as part of its Elastic Cloud services does not store, process, or transmit cardholder data (CHD) in any form. Elastic's customers are responsible for cardholder data stored within their environment.</p> <p>Elastic's Support Service and Cloud service includes infrastructure management, backup and restore, security monitoring, support, maintenance, and connection for customer instances hosted on cloud service providers managed by Elastic Cloud.</p>

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):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Cloud Hosting Provider (PaaS)	19	Google Cloud Platform <ul style="list-style-type: none"> • Taiwan (asia-east1), gcp-asia-east1 • Tokyo (asia-northeast1), gcp-asia-northeast1 • Seoul (asia-northeast3), gcp-asia-northeast3

		<ul style="list-style-type: none"> • Mumbai (asia-south1), gcp-asia-south1 • Singapore (asia-southeast1), gcp-asia-southeast1 • Jakarta (asia-southeast2), gcp-asia-southeast2 • Sydney (australia-southeast1), gcp-australia-southeast1 • Finland (europe-north1), gcp-europe-north1 • Belgium (europe-west1), gcp-europe-west1 • London (europe-west2), gcp-europe-west2 • Frankfurt (europe-west3), gcp-europe-west3 • Netherlands (europe-west4), gcp-europe-west4 • Paris (europe-west9), gcp-europe-west9 • Montreal (northamerica-northeast1), gcp-northamerica-northeast1 • Sao Paulo (southamerica-east1), gcp-southamerica-east1 • Iowa (us-central1), gcp-us-central1 • South Carolina (us-east1), gcp-us-east1 • N. Virginia (us-east4), gcp-us-east4 • Oregon (us-west1), gcp-us-west1
Cloud Hosting Provider (PaaS)	20	<p>Amazon Web Services</p> <ul style="list-style-type: none"> • Tokyo (ap-northeast-1), ap-northeast-1 • Singapore (ap-southeast-1), ap-southeast-1 • Sydney (ap-southeast-2), ap-southeast-2 • Cape Town (af-south-1), aws-af-south-1 • Hong Kong (ap-east-1), aws-ap-east-1 • Seoul (ap-northeast-2), aws-ap-northeast-2 • Mumbai (ap-south-1), aws-ap-south-1 • Canada (ca-central-1), aws-ca-central-1 • Frankfurt (eu-central-1), aws-eu-central-1 • Stockholm (eu-north-1), aws-eu-north-1 • Milan (eu-south-1), aws-eu-south-1

		<ul style="list-style-type: none"> • London (eu-west-2), aws-eu-west-2 • Paris (eu-west-3), aws-eu-west-3 • Bahrain (me-south-1), aws-me-south-1 • Ohio (us-east-2), aws-us-east-2 • Ireland (eu-west-1), eu-west-1 • Sao Paulo (sa-east-1), sa-east-1 • N. Virginia (us-east-1), us-east-1 • N. California (us-west-1), us-west-1 • Oregon (us-west-2), us-west-2
Cloud Hosting Provider (PaaS)	16	Azure <ul style="list-style-type: none"> • New South Wales (australiaeast), azure-australiaeast • Sao Paulo (brazilsouth), azure-brazilsouth • Toronto (canadacentral), azure-canadacentral • Pune (centralindia), azure-centralindia • Iowa (centralus), azure-centralus • Virginia (eastus), azure-eastus • Virginia (eastus2), azure-eastus2 • Paris (francecentral), azure-francecentral • Tokyo (japaneast), azure-japaneast • Ireland (northeurope), azure-northeurope • Johannesburg (southafricanorth), azure-southafricanorth • Texas (southcentralus), azure-southcentralus • Singapore (southeastasia), azure-southeastasia • London (uksouth), azure-uksouth • Netherlands (westeurope), azure-westeurope • Washington (westus2), azure-westus2

Part 2d. Payment Applications

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

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not Applicable	Not Applicable	Not Applicable	<input type="checkbox"/> Yes <input type="checkbox"/> No	Not Applicable

Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

The Elastic Stack comprises a suite of software products that capture and store data from client sources, offering search, analysis, and visualization services. Offered as a subscription-based service, Elastic Cloud is one of Elastic's primary solutions, providing clients with a range of software options such as Search, Observe, and Protect. These can be deployed on-premises, in public or private clouds, or in hybrid setups, catering to diverse user and customer requirements. The product line of Elastic Cloud includes the Elasticsearch Service (ESS) and Elasticsearch Service Private (ESSP).

Elastic Cloud serves as a platform where Elastic oversees and manages components of the Elastic Stack, including Elasticsearch and Kibana, utilizing infrastructure from various public cloud providers like Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. The offerings from Elastic Cloud incorporate advanced features of the Elastic Stack, such as security, alerting, monitoring, reporting, machine learning, and graphing capabilities.

Customers deploying Elastic Cloud have the option to initiate with templates configured for specific use-cases, which include hot-warm architecture, CPU-optimized workloads, I/O optimized workloads, and memory-optimized workloads. Additionally, Elastic Cloud integrates enhanced security features, offering default encryption at rest and support for Security Assertion Markup Language (SAML) and native authentication for hosted deployments.

Elastic's clients have the option to configure their Elastic Cloud deployment and utilize its associated APIs and features to process, manage, and/or store data pertaining to card payments, cardholders, and/or financial transactions involving payment cards. Elastic refrains from accessing customer data unless for explicitly authorized objectives.

Elastic's Cloud service includes infrastructure management, backup and restore, security monitoring, support, maintenance, and connection for customer instances hosted on cloud service providers managed by Elastic Cloud. The PCI assessment's scope is centered on the managed services and supporting technologies that underpin Elastic Cloud's service offering.

Does your business use network segmentation to affect the scope of your PCI DSS environment?

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

Yes No

Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated? Yes No

If Yes:

Name of QIR Company:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable

Does your company have a relationship with one or more 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.) for the purpose of the services being validated? Yes No

If Yes:

Name of service provider:	Description of services provided:
Amazon Web Services, Inc.	Cloud hosting services / Platform as a Service
Google LLC.	Cloud hosting services / Platform as a Service
Microsoft Corporation	Cloud hosting services / Platform as a Service
Okta, Inc.	Single Sign-on and Identity/Access Management Services

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 ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

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 ROC
- 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:		Elasticsearch Service on the Elastic Cloud (ESS) and Elasticsearch Service Private (ESSP)		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req. 1.1.3 – Not Applicable. There is no CDE Req. 1.2.3 – Not Applicable. There are no wireless networks. Req. 1.3.4 – Not Applicable. There is no CDE Req. 1.3.6 – Not Applicable. There are no components that store CHD.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req. 2.1.1 – Not Applicable. There are no wireless networks. Req. 2.2.3 – Not Applicable. There are no insecure services in use. Req. 2.6 – Not Applicable. Elastic is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req. 3.1 – Not Applicable. There are no CHD in scope for this assessment. Req. 3.2 – Not Applicable. There are no CHD in scope for this assessment. Req. 3.3 – Not Applicable. There are no CHD in scope for this assessment. Req. 3.4 – Not Applicable. There are no CHD in scope for this assessment. Req. 3.4.1 – Not Applicable. Disk Encryption is not used.

				Req. 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8 – Not Applicable. There are no key management processes.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req. 4.1 – Not Applicable. There are no transmissions of CHD. Req. 4.1.1 – Not Applicable. There are no wireless networks. Req. 4.2 – Not Applicable. There are no CHD in scope for this assessment. Req. 4.3 – Not Applicable. There are no CHD in scope for this assessment.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req. 8.1.5 – Not Applicable. There are no third-parties with access. Req. 8.7 – Not Applicable. There are no databases with stored CHD in scope.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req. 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2 – Not Applicable. There are no media. Req. 9.9, 9.9.1, 9.9.2, 9.9.3 – Not Applicable. There are no POS/POI devices.
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req. 10.2.1 – Not Applicable. There is not a CDE.
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req. 11.1.1 – Not Applicable. There are no wireless devices. Req. 11.2.3 – Not Applicable. There has not been significant change.
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable A1.1 – Elastic is not a shared hosting provider. A1.2 – Elastic is not a shared hosting provider. A1.3 – Elastic is not a shared hosting provider. A1.4 – Elastic is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable A2.1 – No POS/POI devices within the CDE A2.2 – No POS/POI devices within the CDE A2.3 – No POS/POI devices within the CDE

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	12/11/2023
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 12/11/2023.

Based on the results documented in the ROC 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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Elasticsearch, Inc.</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance: Not Applicable</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td>Not Applicable</td> <td>Not Applicable</td> </tr> <tr> <td>Not Applicable</td> <td>Not Applicable</td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Affected Requirement	Details of how legal constraint prevents requirement being met						
Not Applicable	Not Applicable						
Not Applicable	Not Applicable						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:


(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, 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 my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)


<input checked="" type="checkbox"/>	No evidence of full track data ¹ , CAV2, CVC2, CVN2, CVV2, or CID data ² , or PIN data ³ storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Qualys</i>

Part 3b. Service Provider Attestation

 <small>box SIGN 1JPWV7L1VV665SP</small>	
Signature of Service Provider Executive Officer ↑	Date: 12/11/2023
Service Provider Executive Officer Name: Abby Zumstein	Title: Sr. Manager, Customer Trust and Assurance

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	The QSA performed the assessment and led the effort to document the Report on Compliance. This included: <ul style="list-style-type: none"> • Reviewing pre-assessment evidence for completeness. • Leading on-site assessment to collect and verify evidence in a combination of guided configuration and evidence reviews, application demonstrations, and interviews. • Leading the post on-site remediation and validation process including the review of the evidence for requested sample sets. • Documenting observations based on evidence leading to completion of the Report on Compliance and Attestation of Compliance.
--	--

 <small>box SIGN 42798W7Y1VV665SP</small>	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 12/11/2023
Duly Authorized Officer Name: Kevin Wieting	QSA Company: Coalfire Systems, Inc.

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	<i>Not Applicable</i>
---	-----------------------

¹ Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

² The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

³ Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

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 a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify 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	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting 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"/>	

