



# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Service Providers**

**Version 3.2.1**

June 2018

## 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:	STT Global Data Centres India Pvt. Ltd.		DBA (doing business as):	STT Global Data Centres India Pvt. Ltd.		
Contact Name:	Mr. Shyam Kalamkar		Title:	Associate Director - Certifications Compliance		
Telephone:	+91-9223416212		E-mail:	shyam.kalamkar@sttelemediagdc.in		
Business Address:	Plot No. - C-21 & C-36, "G" BLOCK, Bandra Kurla Complex, Vidyanagari PO		City:	Mumbai		
State/Province:	Maharashtra	Country:	India		Zip:	400 098
URL:	https://www.sttelemediagdc.in					

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

Company Name:	Network Intelligence Pvt. Ltd.				
Lead QSA Contact Name:	Udit Pathak	Title:	PCI-QSA		
Telephone:	+91-7738214202	E-mail:	udit.pathak@niiconsulting.com		
Business Address:	204, Ecospace Tower, 2nd Floor, Off Old Nagardas Road, Andheri East	City:	Mumbai		
State/Province:	Maharashtra	Country:	India	Zip:	400069
URL:	<a href="https://www.niiconsulting.com/">https://www.niiconsulting.com/</a>				

## 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: Co-location Services

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): Not Applicable

**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:

- ☐ 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): Not Applicable

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

Not Applicable

## Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Not applicable.

STT GDC India do not store process and transmit any part of the card holder data as part of there business. Since entity provides colocation services it's customer may have card holder data which is not part of scope of this assessment.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

STT Global Data Centres India Pvt. Ltd. (henceforth to be called as STT GDC India) is a service provider providing datacentre co-location services. STT GDC India does not store, process and/or transmits cardholder data. The scope of the PCI DSS assessment is limited to co-location services (facility and physical security) that they provide to their customers. The scope is finalized assuming the fact that not all customers of STT GDC India are undergoing PCIDSS certification, but

STT GDC India internal infrastructure, people, process and technology are equipped well enough that they can support any of their customers who wish to host any payment card application or infrastructure with STT GDC India at the given inscope locations. Being a data center service provider, STT GDC India by themselves do not store, process or transmit any cardholder data that they own, but any of their customers to whom they are furnishing the services as mentioned above may have cardholder data, which is not in this scope of assessment. STT GDC India customer may have cardholder data, which is stored and processed in their infrastructure hosted with STT GDC India, but may be transmitted over third party internet service providers (Airtel, Reliance, MTNL etc). In-scope are the infrastructure components, people, process and technology, that supports their customers for the services.

## 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>
Data Center	1	Mumbai-BKC: STT Global Data Centres India Pvt. Ltd., Plot C-21 & C-36, 'G' Block, Bandra Kurla Complex, Mumbai 400 098, Maharashtra, INDIA.
Data Center	1	Mumbai-LVSB: STT Global Data Centres India Pvt. Ltd. Lokmanya Videsh Sanchar Bhavan, Kashinath Dhuru Marg, Opp. Kirti College, Prabhadevi, Mumbai – 400 028, Maharashtra, India.
Data Center	1	Pune-Dighi DC1: STT Global Data Centres India Pvt. Ltd. Pune-Alandi Road, Dighi, Pune – 411 015, Maharashtra, India.
Data Center	2	Delhi-GK1 DC1 & DC2 : STT Global Data Centres India Pvt. Ltd. Broadband Tower (DC1) & Nextgen Tower (DC2), Opp. Savitri Cinema

		Flyover, Greater Kailash-1, Delhi – 110 048, India.
Data Center	1	Gujarat-GIFT: STT Global Data Centres India Pvt. Ltd. Building No. 48, Data Centre Building, Gyan Marg, GIFT City, Gandhinagar – 382 355, Gujarat, India.
Data Center	1	Chennai-DC1 (VSB): STT Global Data Centres India Pvt. Ltd. Videsh Sanchar Bhavan, No. 4, Swami Sivananda Salai, Chennai – 600 002, Tamil Nadu, India.
Data Center	1	•Chennai-DC2 (Ambattur): STT Global Data Centres India Pvt. Ltd. 226, Thiruvallur Satellite Earth Station, Red Hills Road, Kallikuppam, Ambattur, Chennai – 600 053, Tamil Nadu, India.
Data Center	1	Bangalore-DC2 (KIADB): STT Global Data Centres India Pvt. Ltd. #18, 19 & 20, EPIP Layout, KIADB, Whitefield, Bengaluru – 560 066, Karnataka, India.
Data Center	1	Bangalore-DC3 (KIADB): STT Global Data Centres India Pvt. Ltd. #142, 143, 144 & 145, EPIP Layout, KIADB, Whitefield, Bengaluru – 560 066, Karnataka, India
Data Center	1	Hyderabad-VSB: STT Global Data Centres India Pvt. Ltd. Videsh Sanchar Bhavan, CFC-1, Software Units Layout, Madhapur, Hyderabad – 500 081, Telangana, India.
Data Center	1	Kolkata-VSB: STT Global Data Centres India Pvt. Ltd. Videsh Sanchar Bhavan, 1/18, C.I.T. Scheme VII-M, Ultadanga, Kolkata – 700 054, West Bengal, India.

## 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 checked="" type="checkbox"/> No	Not Applicable
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

## 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.*

STT GDC India is a datacenter service provider that provides secure facility to host client systems like servers, network devices etc. STT GDC India does not store, process and/or transmits cardholder data. The scope of the PCI DSS assessment is limited to co-location services that they provide to their customers. The scope is finalized assuming the fact that not all customers of STT GDC India are undergoing PCI DSS certification, but STT GDC India internal infrastructure people, process and technology are equipped well enough that they can support any of their customers who wish to host any payment card application or infrastructure with STT GDC India at the given in-scope locations. Being a data center service provider, STT GDC India by themselves do not store, process or transmit any cardholder data that they own, but of their customers to whom they are furnishing the services as mentioned above. STT GDC India customers may have cardholder data, which is not in this scope of assessment, but only those infrastructure components, people, process and technology (physical security) that supports their customers for the services mentioned above is in the scope of assessment.

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:
Not Applicable	Not Applicable

**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:		Co-location Services		
PCI DSS Requirement	Details of Requirements Assessed			
	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:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requirements 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.2.1, 1.2.2, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5,1.3.6, 1.3.7, 1.4,1.5 are not applicable as the scope of the PCI DSS assessment is limited to co-location services that STT GDC INDIA provides to their customers.
Requirement 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requirements 2.1,2.1.1,2.2,2.2.1,2.2.2,2.2.3,2.2.4,2.2.5,2.3,2.4,2.5,2.6 are not applicable as the scope of the PCI DSS assessment is limited to co-location services STT GDC INDIA provides to their customers.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirements 3.1, 3.2, 3.3, 3.4, 3.4.1, 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, 3.7 are not applicable as the scope of the PCI DSS assessment is limited to co-location services that STT GDC INDIA provides to their customers.
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requirements 4.1, 4.1.1, 4.2, 4.3 are not applicable as the scope of the PCI DSS assessment is limited to colocation services that STT GDC INDIA provides to their customers.
Requirement 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requirements 5.1, 5.1.1, 5.1.2, 5.2, 5.3, 5.4 are not applicable as the scope of the PCI DSS assessment

				is limited to co-location services that STT GDC INDIA provides to their customers.
Requirement 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requirements 6.1, 6.2, 6.3, 6.3.1, 6.3.2, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.5.1, 6.4.5.2, 6.4.5.3, 6.4.5.4, 6.4.6, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10, 6.6, 6.7 are not applicable as the scope of the PCI DSS assessment is limited to co-location services that STT GDC INDIA provides to their customers.
Requirement 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requirements 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3, 7.3 are not applicable as the scope of the PCI DSS assessment is limited to co-location services that STT GDC INDIA provides to their customers.
Requirement 8:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requirements 8.1, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.2, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.3.1, 8.3.2, 8.4, 8.5, 8.5.1, 8.6, 8.7, 8.8 are not applicable as the scope of the PCI DSS assessment is limited to co-location services that STT GDC INDIA provides to their customers.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirements 9.5, 9.5.1, 9.6, 9.6.1, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2, 9.9, 9.9.1, 9.9.2, 9.9.3 are not applicable as the scope of the PCI DSS assessment is limited to co-location services that STT GDC INDIA provides to their customers.
Requirement 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requirements 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4, 10.4.1, 10.4.2, 10.4.3, 10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.6.1, 10.6.2, 10.6.3, 10.7, 10.8, 10.8.1, 10.9 are not applicable as the scope of the PCI DSS assessment is limited to co-location services that they provide to their customers.
Requirement 11:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requirements 11.1, 11.1.1, 11.1.2, 11.2, 11.2.1, 11.2.2, 11.2.3, 11.3, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.4.1, 11.4, 11.5, 11.5.1, 11.6 are not applicable as the scope of the PCI DSS assessment is limited to co-location services that they provide to their customers.
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirements 12.3, 12.3.1, 12.3.2, 12.3.3, 12.3.4, 12.3.5, 12.3.6, 12.3.7, 12.3.8, 12.3.9, 12.3.10, 12.5.4, 12.5.5, 12.8, 12.8.1, 12.8.3, 12.8.4, 12.8.5 are not applicable as the scope of the PCI DSS assessment is limited to colocation services that they provide to their customers.

Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable as STT GDC India is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable as STT GDC India is not using SSL/early TLS in their environment

## 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:	14 October 2021	
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 14 October 2021.

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><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby STT Global Data Centres India Pvt. Ltd. has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby <i>(Service Provider Company Name)</i> has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</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><b>Compliant but with Legal exception:</b> 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"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### 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 <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
<input type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Not Applicable

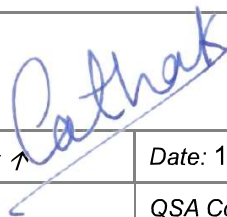
### Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↑	Date: 14 October 2021
Service Provider Executive Officer Name: Sreejith G.	Title: V.P. Data Centre Operations

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA has performed remote and offsite PCI DSS validation for STT Global Data Centres India Pvt. Ltd.
--	---



Signature of Duly Authorized Officer of QSA Company ↑	Date: 14 October 2021
Duly Authorized Officer Name: Udit Pathak	QSA Company: Network Intelligence Pvt. Ltd.

### 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:	Not applicable.
---	-----------------

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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"/>	

