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:	Soft Tech Innovation ltd.		DBA (doing business as):	aamarPay	
Contact Name:	A.M Ishtiaque Sarwar		Title:	Managing Director & Founder	
Telephone:	01711-272324		E-mail:	ishtiaque@aamarpay.com	
Business Address:	Plot 11, Road 2, Sector 3, Paradise Tower, Level-9, Jashimuddin Avenue, Uttara. Dhaka,1230		City:	Dhaka	
State/Province:	Dhaka	Country:	Bangladesh	Zip:	1230
URL:	https://www.softbd.com/				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Enterprise Infosec Consultants				
Lead QSA Contact Name:	Moshiul Islam Mishu		Title:	CEO	
Telephone:	+8801833-182077		E-mail:	moshiul@eic.com.bd	
Business Address:	House 15, Road 7, Block C, Niketan, Gulshan		City:	Dhaka	
State/Province:	Dhaka	Country:	Bangladesh	Zip:	1212
URL:	https://www.eic.com.bd/				

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:	Payment Gateway Service	
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): Payment Gateway Service
☒ 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): Call Center, Merchant Acquisition, Fund Transfer, and QR Acquring		

***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):		
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.	Soft Tech Innovation Ltd. is One Of The Leading Online Payment Gateway & FinTech Company Offering Payment Gateway Solution For SME To Large Enterprises via the aamarPay platform. Soft Tech Innovation Ltd. hereinafter referred as aamarPay is a PSO Licensed online Payment Gateway. Customers who try to pay on a merchant's website are transferred to the aamarPay platform through HTTPS where they can select a payment option. The customer then selects a payment option (debit cards, credit cards, net banking, or mobile wallet). The customer is forwarded to the appropriate bank's or processor's page based on their choice. The customer inputs their card information, including PAN, CVV2, and expiration date, on the bank's processing page. A payment confirmation containing the masked PAN is

	transaction authorization. The masked card information is then returned to the merchant by the aamarPay platform via an API as part of the transaction's confirmation. The first six and last four masked card numbers are kept in the aamarPay database. Additionally, they provide the consumer a payment notification along with the PAN mask, and aamarPay keeps a record of the transactional information for their records. The cardholder's name, expiration date, and masked PAN are stored by aamarPay as part of a recurring transaction. In the course of the process, no sensitive authentication data is being stored. Cardholder name, expiration date, and PAN are stored as encrypted CHD using the AES 256-bit encryption technique. Additionally, a SHA 256 one-time pad is used to save the hashed PAN separately. Through the use of TLS 1.3, aamarPay is connected to their acquirers, who carry out the transaction and provide a success or failure token. The ability to execute recurring transactions with aamarPay is presently limited to City Bank. aamarPay also provides QR scanning service, customer scans the QR code from the merchant application, the request is sent to issuing bank and VISA and UnionPay sends the masked PAN along with the transaction ID to the aamarPay, which is then forwarded to the customer via SMS (payment status confirmation). aamarPay provides customer support regarding the transaction and account related queries using last 4 digits of PAN and mobile number. Call Center application does not process, store or transmit ccardholder data.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not Applicable

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):
Example: Retail outlets	*3*	*Boston, MA, USA*

Head office: Plot 11, Road 2, Sector 3, Paradise Tower, Level-9 Jashimuddin Avenue, Uttara. Dhaka,1230 | Bangladesh	1	Dhaka, Bangladesh
DC: DhakaColo- 10th floor, Khawaja Tower, 95 Bir Uttam AK Khandakar Road, Dhaka 1212	1	Dhaka, Bangladesh
DR: ColoCity- Mohakhali Tower, 82 Mohakhali C/A, Dhaka 1212	1	Dhaka, Bangladesh

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	☐ Yes ☐ No	Not Applicable
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ 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.*	Access control Anti-Virus Logging Monitoring Change Log Failed Attempt Log, IP Restriction Worskstations and Mobile devices Network Devices: Firewalls, WAF Call Center Two Factor Authentication
Does your business use network segmentation to affect the scope of your PCI DSS environment?	☒ Yes ☐ No

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

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:	
Description of services provided by QIR:	
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:	Payment Gateway Service

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:	☒	☐	☐	
Requirement 2:	☐	☒	☐	2.2.3 - Not Applicable [No Insecure services, demons or Protocols are allowed in CDE] 2.6 - Not Applicable [Entity is not a Shared hosting Providers]
Requirement 3:	☐	☒	☐	3.2 - Not Applicale [Entity does not store sensitive authentication Data] 3.6.6 - Not Applicable [Entity does not use manual clear text cryptograpic key management operation]
Requirement 4:	☐	☒	☐	4.1.1 - Not Applicable [Cardholder data is not transmitted through open public wireless network]
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.4.3 - Not Applicale [Live PAN is not used in test enviorment]
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5 - Not Applicable [Remote access for vendor is not allowed in CDE]

				8.5 - Not Applicable [Entity does not use group, shared or generic ID's] 8.5.1 - Not Applicable [Entity does not have POS system or server]
Requirement 9:	☐	☒	☐	9.1.2 - Not Applicable [No publicly accessible jacks are present in CDE] 9.5.1 - Not Applicale [Entity does not have pratice to store media backup in offsite location] 9.6,9.6.1, 9.6.2 , 9.3.3- Not Applicable [Entity does not have pratice to store media ackup in offside location] 9.9,9.9.1, 9.9.2,9.9.3 - Not Applicable[Entity does not have ATM and POS devices]
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	12.3.9, 12.3.10 - Not Applicable [Entity does not provide remote access to venbdor in CDE]
Appendix A1:	☐	☐	☒	Not Applicable [Entity is not a shared hosting provider]
Appendix A2:	☐	☐	☒	Not Applicable [Entity does not have any Card present POS POI Terminal Connections]

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:	7th December 2022	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC 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 the ROC dated 8 December 2022.

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):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Soft Tech Innovation ltd has demonstrated full compliance with the PCI DSS.
☐	**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 *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: 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 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. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

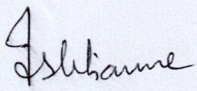
Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	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.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Sectigo

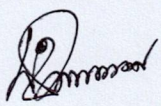
Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↑	*Date:* 7th December 2022
Service Provider Executive Officer Name: A.M Ishtiaque Sarwar	*Title:* Managing Director & Founder

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Moshiul Islam Mishu (PCI QSA) has conducted the assessment and completed the Report on Compliance.



Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 7th December 2022
Duly Authorized Officer Name: Moshiul Islam Mishu	*QSA Company:* Enterprise Infosec Consultants

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

[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	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☐	☒	Entity is not a shared hosting provider
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☒	Entity does not have any Card present POS POI Terminal Connections.