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:	Vindi Tecnologia e Marketing S.A		DBA (doing business as):	VINDI	
Contact Name:	Teógenes Paula Panella Júnior		Title:	Head of Information Security - CISO	
Telephone:	+55 (11) 95271-2707		E-mail:	teogenes.panella@vindi.com.br	
Business Address:	Rua do Paraíso, 148 - Liberdade		City:	São Paulo	
State/Province:	SP	Country:	Brazil	Zip:	04103-000
URL:	https://vindi.com.br				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	AuditSafe Auditoria e Consultoria em Riscos Corporativos Ltda.				
Lead QSA Contact Name:	Fernando Nicolau Freitas Ferreira		Title:	Founder & CEO	
Telephone:	+55 11 2626-1638		E-mail:	fernandoferreira@auditsafe.com.br	
Business Address:	Rua Duarte de Azevedo, 431 – Santana		City:	São Paulo	
State/Province:	SP	Country:	Brazil	Zip:	02036-021
URL:	https://www.auditsafe.com.br				

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	
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:		
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:	N/A.	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	During the audit analysis of the VINDI company, it was observed that it offers online payment infrastructure services through APIs, acting as a payment gateway. Customers have the option of using transparent checkouts. VINDI's environment is hosted in the AWS cloud and the company does not store card data, it only processes and transmits this data. In addition, VINDI works with all credit card brands accepted in the national territory. Through VINDI's APIs, customers can build transparent checkouts and take advantage of the best form of conversion, enabling invisible payments and optimizing checkout performance.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Vindi only transmits and processes the cardholder data, the company does not store cardholder data in its system components. The information that is stored is described in the previous item. Where

	only the first 6 numbers and the last 4 numbers of the card. Vindi is responsible only for providing a network infrastructure for secure capture and transmission, via HTTPs connection, returning a token that represents this card

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*
Amazon AWS	1	Ashburn, VA, USA

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)
Gateway	N/A	Vindi	☐ Yes ☒ No	Not applicable
Recurrent	N/A	Vindi	☐ Yes ☒ No	Not applicable
Vault	N/A	Vindi	☐ Yes ☒ No	Not applicable
			☐ 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).*	This assessment coverd the cloud service technologies(AWS), AWS RDS Database Servers, File Integrity Monitoring (FIM), Tokenization Methods, Host Intrusion Prevention System(HIPS), Operations Systems, Application Servers, Load Balancer Solution, AWS Stateful Security Group, Log Concentrator Solution,

• *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	Vulnerability Scanner Solutions, Web Application Servers, Homegrown Applications, Queue Manager Technologies. Also, it covered a review of the communications: - Vindi to payment gateway using HTTPS with TLSv1.2 with AES 256-bit.
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 Server	Cloud 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:	Payment Gateway

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:	☐	☒	☐	1.2.2 - Not Applicable - There are no routers in the assessed scope. 1.2.3 - Not Applicable - There are no wireless technologies in the assessed scope. 1.3.7 - Not Applicable - There is no Private IP address disclosed. It is not allowed and not configured
Requirement 2:	☐	☒	☐	2.1.1 - Not Applicable - There are no wireless technologies in the assessed scope. 2.2.3 - Not Applicable - There are no insecure services, protocols, or daemons in the assessed scope. 2.6 - Not Applicable - Vindi is not a Shared Service Provider.
Requirement 3:	☐	☒	☐	3.4.1 - Not Applicable - Vindi does not use Disk Encryption for protection of stored cardholder data.
Requirement 4:	☐	☒	☐	4.1.1 - Not Applicable - There are no wireless technologies in the assessed scope.
Requirement 5:	☒	☐	☐	

Requirement 6:	☐	☒	☐	6.5.2 - Not applicable, as our entire platform is developed in Ruby on Rails, which is an uncompiled language.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5 - Not Applicable - Vindi does not provide access in its systems to third parties. 8.5.1 - Not Applicable - Vindi does not provide access in its systems to third parties.
Requirement 9:	☐	☒	☐	9.9 - Not Applicable - Vindi does not use any POS device. 9.9.x - Not Applicable - Vindi does not use any POS device.
Requirement 10:	☐	☒	☐	10.2.7 - Not Applicable – it is not possible to change system objects while online.
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	Not Applicable. Vindi is not a Shared Hosting Provider
Appendix A2:	☐	☐	☒	Not Applicable. Vindi does not use any POS devices.

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:	June 20th, 2023	
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 June 20th, 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):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Vindi Tecnologia e Marketing S.A 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 SERVER SCAN

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↗	*Date:* June 21st, 2023
Service Provider Executive Officer Name: Teógenes Paula Panella Júnior	*Title:* Head of Information Security - CISO

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA performed Quality Assurance of the Report On Compliance

Signature of Duly Authorized Officer of QSA Company ↗	*Date:* June 21st, 2023
Duly Authorized Officer Name: Fernando Nicolau Freitas Ferreira - PCI QSA 205-240	*QSA Company:* AuditSafe Auditoria e Consultoria em Riscos Corporativos Ltda.

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	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	

AUDITSAFE_VINDI-PCI-DSS-v3_2-AOC- 2023.docx

Documento número #5d3b287a-1aed-4b98-9b83-b105f02dfa35

Hash do documento original (SHA256): b72fcbec74de0a4362f9df7cd888834e08822b9e7e3108726d2e3ab7acf8db84

Assinaturas

Fernando Ferreira
Assinou em 21 jun 2023 às 16:15:06

Teogenes de Paula Panella Junior
CPF: 220.454.388-80
Assinou em 21 jun 2023 às 16:53:50

Log

21 jun 2023, 16:11:01	Operador com email matheus.melo@auditsafe.com.br na Conta 42c915e1-3d1a-42d1-bd9b-e3d3c8a8f95f criou este documento número 5d3b287a-1aed-4b98-9b83-b105f02dfa35. Data limite para assinatura do documento: 21 de julho de 2023 (15:56). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
21 jun 2023, 16:11:06	Operador com email matheus.melo@auditsafe.com.br na Conta 42c915e1-3d1a-42d1-bd9b-e3d3c8a8f95f adicionou à Lista de Assinatura: fernandoferreira@auditsafe.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Fernando Ferreira.
21 jun 2023, 16:11:06	Operador com email matheus.melo@auditsafe.com.br na Conta 42c915e1-3d1a-42d1-bd9b-e3d3c8a8f95f adicionou à Lista de Assinatura: teogenes.panella@vindi.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Teogenes de Paula Panella Junior.
21 jun 2023, 16:15:06	Fernando Ferreira assinou. Pontos de autenticação: Token via E-mail fernandoferreira@auditsafe.com.br. IP: 187.90.210.101. Localização compartilhada pelo dispositivo eletrônico: latitude -23.501945668244762 e longitude -46.616999797786626. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.523.0 disponibilizado em https://app.clicksign.com.
21 jun 2023, 16:53:50	Teogenes de Paula Panella Junior assinou. Pontos de autenticação: Token via E-mail teogenes.panella@vindi.com.br. CPF informado: 220.454.388-80. IP: 177.102.248.130. Localização compartilhada pelo dispositivo eletrônico: latitude -22.5656563 e longitude -47.4067218. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.523.0 disponibilizado em https://app.clicksign.com.

21 jun 2023, 16:53:50	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 5d3b287a-1aed-4b98-9b83-b105f02dfa35.