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:	Flexential Corporation		DBA (doing business as):	Flexential	
Contact Name:	David Kidd		Title:	SVP, Governance, Risk and Compliance	
Telephone:	(704) 264-1025		E-mail:	david.kidd@flexential.com	
Business Address:	600 Forest Point Circle, Suite 100		City:	Charlotte	
State/Province:	NC	Country:	USA	Zip:	28273
URL:	https://www.flexential.com				

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

Company Name:	Schellman & Company, LLC				
Lead QSA Contact Name:	Ray Price		Title:	Senior Associate	
Telephone:	866.254.0000 ext. 198		E-mail:	pcirocs@schellman.com	
Business Address:	4010 W Boy Scout Boulevard, Suite 600		City:	Tampa	
State/Province:	FL	Country:	USA	Zip:	33607
URL:	https://www.schellman.com/pci-dss-validation				

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:	Cloud Operations (Managed Compliant Cloud, Client Center Cloud, Hosted Public and Private Cloud)	
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): Compliant Cloud Hosting	**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:	Individual Managed Services, Non-compliant Public and Private Cloud, Professional Services, Colocation	
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): Non-compliant cloud hosting	**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): Professional services		
Provide a brief explanation why any checked services were not included in the assessment:	The scope of this assessment included Flexential's Cloud Operations (Managed Compliant Cloud, Client Center Cloud, Hosted Public and Private Cloud), and Colocation services. All other services were outside the scope of this assessment	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Flexential does not store, process, or transmit any cardholder data within the scope of this PCI DSS assessment.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	This assessment focused on the Cloud Operation service offering which allows clients to maintain and access servers in a dedicated virtual environment in Flexential data centers. Flexential manages the network and hypervisor layers which allow its customers to reduce their employee workload and focus on their operating systems and supporting applications. Flexential's customers are solely responsible for maintaining PCI compliance on their servers. Flexential did not process or have access to any of its customer's cardholder data.

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*
Data Centers	12	744 Roble Road, Allentown, PA 18109 (Allentown) 12655 Edison Dr., Alpharetta, GA, 30005 (Atlanta - Alpharetta) 2775 Northwoods Pkwy, Norcross, GA 30071 (Atlanta - Norcross) 8910 Lenox Pointe Dr, Ste A, G, Charlotte, NC 28273 (Charlotte - South) 3010 Waterview Pkwy, Richardson, TX 75080 (Dallas - Richardson) 11900 E Cornell Ave, Ste A, Aurora, CO 80014 (Denver - Aurora) 8636 South Peoria St, Englewood, CO 80112 (Denver - Englewood) 752 Barret Ave, Louisville, KY 40204 (Louisville - Downtown) 3500 Lyman Blvd, Chaska, MN 55318 (Minneapolis - Chaska) 425 Duke Dr, Ste 400, Franklin, TN 37067 (Nashville - Cool Springs) 5737 NE Huffman Street, Hillsboro OR 97124 (Portland - Hillsboro 2) 572 Delong St, Ste 100, Salt Lake City, UT 84104 (Salt Lake City - Downtown)
Third party data centers	Two (2)	Luttenbergweg 4, 1101 EC Amsterdam, Netherlands (Equinix) 2001 6th Ave., Seattle, WA 98121 (The Westin Building)

Part 2c. Locations

Cloud Hosting Provider	One (1)	US-East-1 (Amazon Web Services)

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.	N/A	N/A	☐ Yes ☐ 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.*	Flexential manages the underlying network and infrastructure to host customer virtual machines which may or may not store, process, or transmit cardholder data. The core system components supporting the service include: - Fortinet firewalls - VMware ESXi servers, vCenter - Windows servers - Red Hat Enterprise Linux - NetApp and Infinidat storage appliances
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	Cloud service provider	
BAE SilverSky	Network monitoring	
Digital Realty	Colocation provider	
Equinix	Colocation provider	
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:	Cloud Operations (Managed Compliant Cloud, Client Center Cloud, Hosted Public and Private Cloud)

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:	☐	☒	☐	1.1.3: Not applicable. Flexential did not process, store, or transmit cardholder data. Flexential's customers were responsible for meeting this requirement. 1.2.3: Not applicable. There were no wireless networks directly connected to the cardholder data environment 1.3.6: Not applicable. Flexential did not store cardholder data in the scope of this assessment.
Requirement 2:	☐	☒	☐	2.1.1: Not applicable. There were no wireless networks within or connected to the CDE. 2.2.3: Not applicable. There were no insecure services observed in the CDE.
Requirement 3:	☐	☒	☐	Not applicable. Flexential did not store, process, or transmit any cardholder data. The only applicable requirements in this section were 3.2.1, 3.2.2, and 3.2.3.
Requirement 4:	☐	☐	☒	Not applicable. Flexential did not transmit any cardholder data in the scope of this assessment.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.4.6: Not applicable. There were no significant changes in the 12 months preceding the assessment.
Requirement 7:	☒	☐	☐	

Requirement 8:	☐	☒	☐	8.1.5: Not applicable. Observed the access control lists for the CDE systems and noted that no vendor accounts existed on any systems. 8.5.1: Not applicable, Flexential did not have remote access to customer systems in the scope of this assessment. 8.7: Not applicable. Flexential did not maintain any databases which stored cardholder data in the scope of this assessment.
Requirement 9:	☐	☒	☐	9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8: Not applicable. Flexential did not perform backups to removable media or have access to any credit card numbers. 9.8.1: Not applicable. Flexential did not maintain any hard-copy materials containing cardholder data. 9.8.2: Not applicable. Flexential did not store any credit card numbers anywhere in the HPC environment. 9.9, 9.9.1, 9.9.2, 9.9.3: Not applicable. Flexential did not maintain any payment card interaction devices.
Requirement 10:	☐	☒	☐	10.2.1: Not applicable. Flexential did not store cardholder data in relation to the in-scope environment.
Requirement 11:	☐	☒	☐	11.1.1: Not applicable, there were no wireless access points connected to the CDE. 11.2.3: Not applicable. There were no significant changes in the last 12 months.
Requirement 12:	☐	☒	☐	12.3.9: Not applicable. Observed the access control lists for the CDE systems and noted that no vendor accounts existed on any systems 12.3.10: Not applicable. Flexential did not store or have access to cardholder data in the scope of this assessment.
Appendix A1:	☐	☒	☐	A1.3: Not applicable. Flexential customers were responsible for this requirement.
Appendix A2:	☐	☐	☒	Not applicable. Flexential did not maintain any POS/POI devices or use SSL/early TLS within the scope of the colocation services 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:	*November 15, 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 *November 15, 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 *Flexential Corporation* 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 *Flexential Corporation* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: N/A 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
N/A	N/A

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 *Tenable.*

Part 3b. Service Provider Attestation

DocuSigned by:
David A. Kidd
4D326E09C4B94CB...

Signature of Service Provider Executive Officer ↑	*Date:* 12/16/2022
Service Provider Executive Officer Name: **David Kidd**	*Title:* **Senior Vice President, Governance, Risk and Compliance**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Independent Assessor

DocuSigned by:
980C45A0461544C...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 12/16/2022
Duly Authorized Officer Name: Douglas W. Barbin	*QSA Company:* Schellman & Company, LLC

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