



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 & 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:	Daniel Garczek	Title:	Senior Associate		
Telephone:	866.254.0000 ext. 476	E-mail:	pciocs@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:

Colocation

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: Cloud Operations (Managed Compliant Cloud, Client Center Cloud, Hosted Public and Private Cloud)

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:

This service was covered by this PCI DSS assessment but has a separate AOC.

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.

Flexential operates colocation facilities whereby their customers rent space for customers' systems and connectivity to the broader Internet. All access to systems and data are the responsibility of the customers themselves. Flexential simply provides secure space, power, and environmental controls for merchants and service providers, some of which fall under PCI compliance.

Flexential has no logical access to any customer systems that may contain cardholder data and their managed services are not in the scope of this assessment.

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>
Colocation	38	744 Roble Road, Allentown, PA 18109 (Allentown) 12655 Edison Dr., Alpharetta, GA, 30005 (Atlanta - Alpharetta) 2775 Northwoods Pkwy, Norcross, GA 30071 (Atlanta - Norcross) 10105 David Taylor Dr., Charlotte, NC, 28262 (Charlotte - North) 8910 Lenox Pointe Dr, Ste A, G, Charlotte, NC 28273 (Charlotte - South) 5307 Muhlhauser Rd, West Chester Township, OH 45011 (Cincinnati) 101 Troutman Rd., Collegeville, PA 19426 (Collegeville) 1950 N Stemmons Fwy, Dallas, TX 75207 (Dallas - Downtown) 3500 E Plano Pkwy, Plano, TX 75074 (Dallas - Plano) 3010 Waterview Pkwy, Richardson, TX 75080 (Dallas - Richardson) 11900 E Cornell Ave, Ste A, Aurora, CO 80014 (Denver - Aurora) 12500 E Arapahoe Rd, Ste C, Centennial, CO 80112 (Denver - Centennial) 1500 Champa St, Ste 100, Denver, CO 80202 (Denver - Downtown) 8636 South Peoria St, Englewood, CO 80112 (Denver - Englewood) 5301 NW 33rd Ave, Fort Lauderdale, FL 33309 (Fort Lauderdale) 4905 Belfort Rd, Ste 145, Jacksonville, FL 32256 (Jacksonville) 302 East Carson Ave, Ste 100, Las Vegas, NV 89101 (Las Vegas - Downtown 1) 304 East Carson Ave, Las Vegas, NV 89101 (Las Vegas - Downtown 2) 3330 E Lone Mountain Rd, North Las Vegas, NV 89081 (Las Vegas - North) 752 Barret Ave, Louisville, KY 40204 (Louisville - Downtown) 2101 Nelson Miller Pkwy, Louisville, KY 40223 (Louisville - East) 3500 Lyman Blvd, Chaska, MN 55318 (Minneapolis - Chaska)

Part 2c. Locations

		<p>7100 Commerce Way, Brentwood, TN 37027 (Nashville - Brentwood)</p> <p>425 Duke Dr, Ste 400, Franklin, TN 37067 (Nashville - Cool Springs)</p> <p>4600 Carothers Pkwy, Franklin, TN 37067 (Nashville - Franklin)</p> <p>1850 W. Deer Valley Rd, Phoenix, AZ 85027 (Phoenix - Deer Valley)</p> <p>3935 NW Aloclek Pl, Bldg C, Hillsboro, OR 97124 (Portland - Hillsboro 1)</p> <p>5737 NE Huffman Street, Hillsboro OR 97124 (Portland - Hillsboro 2)</p> <p>5150 McCrimmon Parkway, Morrisville, NC 27560 (Raleigh)</p> <p>8851 Park Central Dr, Richmond, VA 23227 (Richmond)</p> <p>6340 S 3000 E, Ste 150, Salt Lake City, UT 84121 (Salt Lake City - Cottonwood)</p> <p>572 Delong St, Ste 100, Salt Lake City, UT 84104 (Salt Lake City - Downtown)</p> <p>118 S 1000 W, Salt Lake City, UT 84104 (Salt Lake City - Fair Park)</p> <p>333 S 520 W, Lindon, UT 84042 (Salt Lake City - Lindon)</p> <p>3949 S 200 E, Murray, UT 84107 (Salt Lake City - Millcreek)</p> <p>7202 S Campus View Dr, West Jordan, UT 84084 (Salt Lake City - South Valley)</p> <p>8350 Parkedge Dr., Tampa, FL, 33637 (Tampa - North)</p> <p>9417 Corporate Lake Dr, Tampa, FL 33634 (Tampa - West)</p>
--	--	--

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).*

Flexential's colocation services environment included physical security of the listed data centers and the badge access system that controlled access to those data centers. Policies and procedures around access

<ul style="list-style-type: none">• <i>Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.</i>	control, physical security, and incident response were also assessed.
Does your business use network segmentation to affect the scope of your PCI DSS environment? <i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
---	---

If Yes:

Name of service provider:	Description of services provided:
----------------------------------	--

Allied	Security guards at data centers
--------	---------------------------------

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:		Colocation		
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"/>	Not applicable. Based on the scope of services, Flexential customers were responsible for complying with this requirement.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1: Not applicable. Based on the scope of services, Flexential customers are responsible for complying with this requirement. 2.2.3: Not applicable. No insecure services were observed within the environment. 2.6: Not applicable. Flexential was not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.1 – 3.2, 3.3 – 3.7: Not applicable. Based on the scope of services, Flexential customers were responsible for complying with this requirement.
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not applicable. Based on the scope of services, Flexential customers were responsible for complying with this requirement.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.3-6.3.2, 6.4.1-6.4.4, 6.4.6.4-6.6: Not applicable. Based on the scope of services, Flexential customers were responsible for complying with this requirement. 6.4.6: Not applicable. There were no significant changes in the 12 months preceding the assessment.
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.1.5: Not applicable. Flexential did not permit vendors to have remote access to in-scope systems. 8.5.1: Not applicable. Flexential did not have remote access to customer premises. 8.7: Not applicable. Flexential did not store cardholder data within the scope of the colocation services environment.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.5 - 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 cardholder data within the scope of the colocation services environment. 9.9 - 9.9.3: Not applicable. Flexential did not maintain any payment card interaction devices.
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.2.1: Not applicable. Flexential did not store cardholder data within the scope of the colocation services environment.
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.1 – 11.4: Not applicable. Based on the scope of services, Flexential customers were responsible for complying with this requirement.
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.3.9: Not applicable. Flexential did not permit vendors to have remote access to in-scope systems. 12.3.10: Not applicable. Flexential did not have any access to cardholder data within the scope of the colocation services environment.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not applicable. Flexential was not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	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:	<i>November 15, 2021</i>
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes <input 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 **November 15, 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>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Flexential Corporation</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>Flexential Corporation</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"> <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></td> </tr> <tr> <td></td> <td></td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met	Not applicable.			
Affected Requirement	Details of how legal constraint prevents requirement being met						
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, Version (version number)</i> , 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)


- No evidence of full track data¹, CAV2, CVC2, CID, or CVV2 data², or PIN data³ 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 *Not applicable*.

Part 3b. Service Provider Attestation

DocuSigned by: 	
4D326E09C4B94CB... Signature of Service Provider Executive Officer ↑	Date: 12/3/2021
Service Provider Executive Officer Name: David Kidd	Title: Senior Vice President, Governance, Risk & 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: 	
8BF609729B1942F... Signature of Duly Authorized Officer of QSA Company ↑	Date: 12/3/2021
Duly Authorized Officer Name: Debbie Zaller	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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.

