PCI Security Standards Council®

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:	Microsoft SharePoint Online and OneDrive for Business	DBA (doing business as):	N/A		
Contact Name:	Melodi Crowley	Title:	Principal Program Manager Lead		
Telephone:	(425) 880-8080	E-mail:	Melodi.crowley@microsoft.com		
Business Address:	One Microsoft Way	City:	Redmond		
State/Province:	WA	Country:	USA	Zip:	98052
URL:	https://www.microsoft.com				

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

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Allen Mahaffy	Title:	Practice Director		
Telephone:	(303) 554-6333	E-mail:	CoalfireSubmission@coalfire.com		
Business Address:	11000 Westmoor Cir Ste 450	City:	Westminster		
State/Province:	CO	Country:	USA	Zip:	80021
URL:	https://www.coalfire.com				

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:	Microsoft SharePoint Online and OneDrive for Business	
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:	None

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.	Microsoft Office 365 (O365) does not directly store, process or transmit cardholder data (CHD). O365 offers SharePoint Online and OneDrive for business as Software as a Service (SaaS) to customers who may store or transmit cardholder data (CHD) in their allocated resources.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Microsoft O365 is a SaaS service provider, offering SharePoint Online (SPO), and OneDrive for Business (ODB) services to customers of all sizes. SPO and/or ODB customers, or subscribers, may store or transmit CHD in their allocated environments. Subscribers are responsible for all applicable PCI requirements pertaining to CHD handling in transit or at rest, whereas, O365 is responsible for SPO and ODB system components' applicable PCI requirements. SPO and ODB infrastructure is hosted and managed by Microsoft Azure, a Level 1 PCI-DSS compliant Service Provider as validated by AOC version 3.2.1, dated 03/01/2019.

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):
Microsoft Azure Data Center	1	Blue Ridge, VA
Microsoft Azure Data Center	1	Boydton, VA
Microsoft Azure Data Center	1	Chicago, IL
Microsoft Azure Data Center	1	Des Moines, IA
Microsoft Azure Data Center	1	San Antonio, TX

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

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.*	The SPO & ODB environment operates within Azure's infrastructure and IaaS from multiple services. All connections into the hosted environment are over TLS 1.2 to front-end load balancers and web server. Data is stored using Azure SQL and Azure Blob Storage. Customers have the ability to encrypt data with Azure Key Vault. Critical components include both bare metal and virtual Win 2012 and Win 2016 server. All network devices are owned and managed by Azure.
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:**
Microsoft Azure	Azure provides Infrastructure as a Service (IaaS), Colocation services, and network devices management.
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:	Microsoft SharePoint Online and OneDrive for Business			
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:	☐	☒	☐	2.1.1 – N/A – No wireless networks inside the scoped environment.
Requirement 3:	☐	☒	☐	3.1, 3.2, 3.3, – N/A – SPO & ODB does not directly store, process or transmit CHD. All CHD handling requirements are the customers’ responsibilities.
Requirement 4:	☐	☒	☐	4.1.1 – N/A – no wireless, or connections to wireless networks in scope. 4.2– N/A – no end-user messaging technologies in use.
Requirement 5:	☐	☒	☐	5.1.2 – N/A – No systems considered to be not commonly affected by malicious malware in scoped environment.
Requirement 6:	☐	☒	☐	6.4.3 – N/A - SPO & ODB does not directly store, process or transmit CHD and no testing. 6.4.6 – N/A – No significant change has occurred in the past 12 months
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5 – N/A – No third-parties remote access is allowed into the CDE.

				8.5.1, 8.6 – N/A – SPO & ODB service teams don't have remote access into the customer environment. 8.7 – N/A - SPO & ODB does not directly store, process or transmit CHD.
Requirement 9:	□	☒	□	9.9, 9.9.1, 9.9.2, 9.9.3 – N/A – SPO & ODB does not own/maintain POS devices
Requirement 10:	□	☒	□	10.2.1 – N/A – SPO & ODB does not directly store, process or transmit CHD.
Requirement 11:	□	☒	□	11.2.3 – N/A – No significant change has occurred in the past 12 months
Requirement 12:	□	☒	□	12.3.9, 12.3.10 – N/A - SPO & ODB does not directly store, process or transmit CHD or allow vendors access.
Appendix A1:	□	□	☒	A1.1, A1.2, A1.3, A1.4 - N/A - SPO & ODB is not a shared hosting provider.
Appendix A2:	□	□	☒	A2.1 – N/A - SPO & ODB does not directly process any card-present transactions from any system including point-of-sale (POS) devices. A2.2 – N/A - SPO & ODB does not directly process any card-present transactions from any system including point-of-sale (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:	7/19/2019	
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 *7/19/2019.*

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 Microsoft SharePoint Online and OneDrive for Business 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 *N/A* 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 *Qualys (Certificate number 3728-01-13)*

Part 3b. Service Provider Attestation

DocuSigned by:
Melodi Crowley
2C1024F4558B42A...

Signature of Service Provider Executive Officer ↑	*Date:* **8/12/2019**
Service Provider Executive Officer Name: **Melodi Crowley**	*Title:* **Principal Program Manager Lead**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	Conducted PCI DSS v3.2.1 remote and onsite assessment and documented compliance results in the Report on Compliance (ROC) and the associated Attestation of Compliance (AOC).

DocuSigned by:
Allen Mahaffy
5900E9D972AA44B...

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 8/12/2019*
Duly Authorized Officer Name: **Allen Mahaffy**	*QSA Company:* **Coalfire Systems, Inc.**

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:	N/A

[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	☒	☐	

AMERICAN EXPRESS DISCOVER JCB mastercard VISA