



# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Service Providers**

**Version 3.2**

April 2016

## 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:     | Peak 10, Inc.   | DBA (doing business as): | Peak 10  |      |       |
| Contact Name:     | David Kidd  | Title:                   | Vice President of Governance, Risk, and Compliance |      |       |
| Telephone:        | 704.264.1025  | E-mail:                  | David.Kidd@Peak10.com                              |      |       |
| Business Address: | 8810 Lenox Pointe Drive, Suite G                          | City:                    | Charlotte  |      |       |
| State/Province:   | NC  | Country:                 | USA  | Zip: | 28273 |
| URL:              | <a href="http://www.peak10.com">http://www.peak10.com</a> |                          |  |      |       |

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

|                        |   |          |                            |      |       |
|------------------------|---|----------|----------------------------|------|-------|
| Company Name:          | Schellman & Company, LLC  |          |                            |      |       |
| Lead QSA Contact Name: | Matt Crane  | Title:   | Senior Associate           |      |       |
| Telephone:             | 866.254.0000 ext. 174   | E-mail:  | matt.crane@schellmanco.com |      |       |
| Business Address:      | 4010 W Boy Scout Boulevard, Suite 600   | City:    | Tampa                      |      |       |
| State/Province:        | FL  | Country: | USA                        | Zip: | 33607 |
| URL:                   | <a href="https://www.schellman.com/pci-dss-validation">https://www.schellman.com/pci-dss-validation</a> |          |                            |      |       |

## 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:   |   | Data Center Operations and Managed Cloud Services  |  |
| Type of service(s) assessed:   |   |  |  |
| <b>Hosting Provider:</b><br><input type="checkbox"/> Applications / software<br><input type="checkbox"/> Hardware<br><input type="checkbox"/> Infrastructure / Network<br><input checked="" type="checkbox"/> Physical space (co-location)<br><input type="checkbox"/> Storage<br><input type="checkbox"/> Web<br><input type="checkbox"/> Security services<br><input type="checkbox"/> 3-D Secure Hosting Provider<br><input checked="" type="checkbox"/> Shared Hosting Provider<br><input type="checkbox"/> Other Hosting (specify): | <b>Managed Services (specify):</b><br><input checked="" type="checkbox"/> Systems security services<br><input type="checkbox"/> IT support<br><input type="checkbox"/> Physical security<br><input type="checkbox"/> Terminal Management System<br><input type="checkbox"/> Other services (specify): | <b>Payment Processing:</b><br><input type="checkbox"/> POS / card present<br><input type="checkbox"/> Internet / e-commerce<br><input type="checkbox"/> MOTO / Call Center<br><input type="checkbox"/> ATM<br><input type="checkbox"/> Other processing (specify): |  |
| <input type="checkbox"/> Account Management  | <input type="checkbox"/> Fraud and Chargeback   | <input type="checkbox"/> Payment Gateway/Switch  |  |
| <input type="checkbox"/> Back-Office Services  | <input type="checkbox"/> Issuer Processing  | <input type="checkbox"/> Prepaid Services  |  |
| <input type="checkbox"/> Billing Management  | <input type="checkbox"/> Loyalty Programs   | <input type="checkbox"/> Records Management  |  |
| <input type="checkbox"/> Clearing and Settlement   | <input type="checkbox"/> Merchant Services  | <input type="checkbox"/> Tax/Government Payments   |  |
| <input type="checkbox"/> Network Provider  |   |  |  |
| <input type="checkbox"/> 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: Managed Services other than Cloud Services

Type of service(s) not assessed:

| <b>Hosting Provider:</b>   | <b>Managed Services (specify):</b>   | <b>Payment Processing:</b>   |
|--|--|--|
| <input type="checkbox"/> Applications / software<br><input type="checkbox"/> Hardware<br><input type="checkbox"/> Infrastructure / Network<br><input type="checkbox"/> Physical space (co-location)<br><input type="checkbox"/> Storage<br><input type="checkbox"/> Web<br><input type="checkbox"/> Security services<br><input type="checkbox"/> 3-D Secure Hosting Provider<br><input type="checkbox"/> Shared Hosting Provider<br><input type="checkbox"/> Other Hosting (specify): | <input checked="" type="checkbox"/> Systems security services<br><input checked="" type="checkbox"/> IT support<br><input type="checkbox"/> Physical security<br><input type="checkbox"/> Terminal Management System<br><input type="checkbox"/> Other services (specify): | <input type="checkbox"/> POS / card present<br><input type="checkbox"/> Internet / e-commerce<br><input type="checkbox"/> MOTO / Call Center<br><input type="checkbox"/> ATM<br><input type="checkbox"/> Other processing (specify): |
| <input type="checkbox"/> Account Management  | <input type="checkbox"/> Fraud and Chargeback  | <input type="checkbox"/> Payment Gateway/Switch  |
| <input type="checkbox"/> Back-Office Services  | <input type="checkbox"/> Issuer Processing   | <input type="checkbox"/> Prepaid Services  |
| <input type="checkbox"/> Billing Management  | <input type="checkbox"/> Loyalty Programs  | <input type="checkbox"/> Records Management  |
| <input type="checkbox"/> Clearing and Settlement   | <input type="checkbox"/> Merchant Services   | <input type="checkbox"/> Tax/Government Payments   |
| <input type="checkbox"/> Network Provider  |  |  |
| <input type="checkbox"/> Others (specify):   |  |  |

Provide a brief explanation why any checked services were not included in the assessment:

Peak 10 customers have the ability to administer their own guest systems so while Peak 10 may perform these services, the customer could potentially undo any of the configuration changes

**Part 2b. Description of Payment Card Business**

|  |  |
|--|--|
| Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.                                   | Not applicable, for the purposes of this assessment. Peak 10 did not store, process, transmit or maintain cardholder data and has no logical access to any customer system that may contain cardholder data.   |
| Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data. | <p>Peak 10 provides colocation and cloud services to clients. Peak 10's colocation services allow clients to rent server rack space for server and infrastructure components. All configuration and management of the systems is the clients responsibility. Peak 10 provides physical security, electricity, environmental controls, and Internet connectivity only. Some of these controls fall under PCI compliance.</p> <p>Cloud computing services allow clients to maintain and access server and infrastructure components in a dedicated virtual environment in Peak 10 data centers. Peak 10 provides supporting infrastructure to clients including all the services provided in the colocation services and adds secure remote connections and management of hypervisors and associated hardware. Customers are still responsible for managing their own systems.</p> |

**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>  |
| Data Centers                   | 25                                | Norcross, GA USA<br>Alpharetta, GA USA<br>Charlotte, NC USA<br>Hamilton, OH USA<br>Jacksonville, FL USA<br>Louisville, KY USA<br>Brentwood, TN USA<br>Franklin, TN USA<br>Morrisville, NC USA<br>Richmond, VA USA<br>Fort Lauderdale, FL USA<br>Tampa, FL 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) |
|--------------------------|----------------|--------------------|--|--|
|                          |                |                    | <input type="checkbox"/> Yes <input type="checkbox"/> No |  |
|                          |                |                    | <input type="checkbox"/> Yes <input type="checkbox"/> No |  |
|                          |                |                    | <input type="checkbox"/> Yes <input type="checkbox"/> No |  |
|                          |                |                    | <input type="checkbox"/> Yes <input type="checkbox"/> No |  |
|                          |                |                    | <input type="checkbox"/> Yes <input type="checkbox"/> No |  |
|                          |                |                    | <input type="checkbox"/> Yes <input type="checkbox"/> No |  |
|                          |                |                    | <input type="checkbox"/> Yes <input type="checkbox"/> No |  |
|                          |                |                    | <input type="checkbox"/> Yes <input type="checkbox"/> 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.*

Management infrastructure utilized to manage customer cloud environments which may or may not store, process, or transmit cardholder data. Additionally, colocation services for customers. Peak 10 utilizes FortiGate firewalls, Windows servers, and VMware ESXi servers to manage the cloud infrastructure.

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:

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:  |
|---------------------------|--|
| BAE Systems               | Intrusion Detection / Prevention Monitoring and Management<br>Centralized Log Management and Monitoring<br>File Integrity Monitoring<br>Vulnerability Scanning |
|                           |  |
|                           |  |
|                           |  |
|                           |  |

**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: |                                     | Data Center Operations and Managed Cloud Services |                                     |  |
|---------------------------|-------------------------------------|---|-------------------------------------|--|
| PCI DSS Requirement       | Details of Requirements Assessed    |   |                                     | Justification for Approach<br>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)   |
|                           | Full                                | Partial   | None                                |  |
| Requirement 1:            | <input type="checkbox"/>            | <input checked="" type="checkbox"/>               | <input type="checkbox"/>            | <b>1.1.3-Peak 10 customers were responsible for cardholder data flow diagrams</b><br><b>1.2.3-No wireless connections to the environment</b><br><b>1.3.7-Peak 10 does not store cardholder data</b>  |
| Requirement 2:            | <input type="checkbox"/>            | <input checked="" type="checkbox"/>               | <input type="checkbox"/>            | <b>2.1.1-No wireless connections to the environment</b><br><b>2.2.3-No wireless connections to the environment</b>   |
| Requirement 3:            | <input type="checkbox"/>            | <input checked="" type="checkbox"/>               | <input type="checkbox"/>            | <b>All of requirement 3 except for 3.2.1, 3.2.2, and 3.2.3-Peak 10 did not store, process, or transmit cardholder data</b>   |
| Requirement 4:            | <input type="checkbox"/>            | <input type="checkbox"/>                          | <input checked="" type="checkbox"/> | <b>Peak 10 did not store, process, or transmit cardholder data.</b>  |
| Requirement 5:            | <input checked="" type="checkbox"/> | <input type="checkbox"/>                          | <input type="checkbox"/>            |  |
| Requirement 6:            | <input type="checkbox"/>            | <input checked="" type="checkbox"/>               | <input type="checkbox"/>            | <b>6.3-6.6 except for 6.4.5-Peak 10 did not develop software applications that stored, processed, or transmitted cardholder data.</b><br><b>6.4.6-Peak 10 has not yet implemented this best practice, yet future dated requirement, as of this assessment.</b> |
| Requirement 7:            | <input checked="" type="checkbox"/> | <input type="checkbox"/>                          | <input type="checkbox"/>            |  |



|                 |                          |                                     |                                     |   |
|-----------------|--------------------------|-------------------------------------|-------------------------------------|---|
| Requirement 8:  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <p><b>8.1.5-Peak 10 does not have any vendors or third parties that access systems in the CDE.</b></p> <p><b>8.3.1, 8.5.1-Peak 10 has not yet implemented this best practice, yet future dated requirement, as of this assessment.</b></p> <p><b>8.7-Peak 10 did not maintain any databases which stored cardholder data.</b></p> |
| Requirement 9:  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <p><b>9.1.2-There were no publicly accessible network jacks</b></p> <p><b>9.5-9.8-Peak 10 did not maintain any media containing cardholder data. Backup services were not included in the assessment.</b></p> <p><b>9.9-Peak 10 did not maintain any card reading devices</b></p>   |
| Requirement 10: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <p><b>10.2.1-It is the customers responsibility to log access to CHD.</b></p> <p><b>10.8, 10.8.1-Peak 10 has not yet implemented this best practice, yet future dated requirement, as of this assessment.</b></p>   |
| Requirement 11: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <p><b>11.1.1-No wireless connections were allowed to connect to the environment.</b></p> <p><b>11.2.3-No significant changes occurred in the last 12 months</b></p> <p><b>11.3.4.1-Peak 10 has not yet implemented this best practice, yet future dated requirement, as of this assessment.</b></p>                               |
| Requirement 12: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <p><b>12.4.1, 12.11, 12.11.1-Peak 10 has not yet implemented this best practice, yet future dated requirement, as of this assessment.</b></p>   |
| Appendix A1:    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <p><b>A.1.3-Peak 10 customers were responsible for complying with logging requirements as they had the ability to enable logging on their exclusive virtual environment via the BAE Systems log management service</b></p>  |
| Appendix A2:    | <input type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <p><b>Peak 10 did not have any instances of or support the use of SSL or early TLS.</b></p>   |

## 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: | 01/08/2018                              |  |
| 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 *January 8, 2018*.

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><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>Peak 10</i> has demonstrated full compliance with the PCI DSS.</p>  |                      |  |  |  |  |  |
|-------------------------------------|--|----------------------|--|--|--|--|--|
| <input type="checkbox"/>            | <p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</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><b>Compliant but with Legal exception:</b> 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" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table> | Affected Requirement | Details of how legal constraint prevents requirement being met |  |  |  |  |
| Affected Requirement                | Details of how legal constraint prevents requirement being met   |                      |  |  |  |  |  |
|                                     |  |                      |  |  |  |  |  |
|                                     |  |                      |  |  |  |  |  |

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

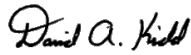
(Check all that apply)

|                                     |   |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2, 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 data<sup>1</sup>, CAV2, CVC2, CID, or CVV2 data<sup>2</sup>, or PIN data<sup>3</sup> 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*

**Part 3b. Service Provider Attestation**



|  |  |
|--|--|
| <i>Signature of Service Provider Executive Officer</i> ↑   | <i>Date:</i> Jan 15, 2018  |
| <i>Service Provider Executive Officer Name:</i> David Kidd | <i>Title:</i> Vice President of 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: | <i>Independent Assessor</i> |
|--|-----------------------------|



Douglas Barbin (Jan 15, 2018)

|  |  |
|--|--|
| <i>Signature of Duly Authorized Officer of QSA Company</i> ↑ | <i>Date:</i> Jan 15, 2018                    |
| <i>Duly Authorized Officer Name:</i> Douglas W. Barbin       | <i>QSA Company:</i> 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: |  |
|---|--|

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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<br>(Select One) |                          | Remediation Date and Actions<br>(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"/> |  |
| 2                   | Do not use vendor-supplied defaults for system passwords and other security parameters   | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 3                   | Protect stored cardholder data   | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 4                   | Encrypt transmission of cardholder data across open, public networks                     | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 5                   | Protect all systems against malware and regularly update anti-virus software or programs | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 6                   | Develop and maintain secure systems and applications                                     | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 7                   | Restrict access to cardholder data by business need to know                              | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 8                   | Identify and authenticate access to system components                                    | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 9                   | Restrict physical access to cardholder data  | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 10                  | Track and monitor all access to network resources and cardholder data                    | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 11                  | Regularly test security systems and processes  | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| 12                  | Maintain a policy that addresses information security for all personnel                  | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| Appendix A1         | Additional PCI DSS Requirements for Shared Hosting Providers                             | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |
| Appendix A2         | Additional PCI DSS Requirements for Entities using SSL/early TLS                         | <input checked="" type="checkbox"/>               | <input type="checkbox"/> |  |





# Peak10 - 2018 PCI DSS - AOC Service Providers

Adobe Sign Document History

01/15/2018

|                 |  |
|-----------------|--|
| Created:        | 01/15/2018                                   |
| By:             | Douglas Barbin (doug.barbin@schellmanco.com) |
| Status:         | Signed                                       |
| Transaction ID: | CBJCHBCAABAA15bVGWsqxbhHICRtEYqedAudn1SIWhGi |

## "Peak10 - 2018 PCI DSS - AOC Service Providers" History

- Document created by Douglas Barbin (doug.barbin@schellmanco.com)  
01/15/2018 - 9:52:01 AM PST- IP address: 8.36.116.253
- Document emailed to David Kidd (david.kidd@peak10.com) for signature  
01/15/2018 - 9:53:02 AM PST
- Document viewed by David Kidd (david.kidd@peak10.com)  
01/15/2018 - 9:55:23 AM PST- IP address: 66.129.64.222
- Document e-signed by David Kidd (david.kidd@peak10.com)  
Signature Date: 01/15/2018 - 9:55:51 AM PST - Time Source: server- IP address: 66.129.64.222
- Document emailed to Douglas Barbin (doug.barbin@schellmanco.com) for signature  
01/15/2018 - 9:55:52 AM PST
- Document viewed by Douglas Barbin (doug.barbin@schellmanco.com)  
01/15/2018 - 9:56:39 AM PST- IP address: 8.36.116.254
- Document e-signed by Douglas Barbin (doug.barbin@schellmanco.com)  
Signature Date: 01/15/2018 - 9:57:24 AM PST - Time Source: server- IP address: 8.36.116.252
- Signed document emailed to debbie.zaller@schellman.com, kim.wright@viawest.com, Douglas Barbin (doug.barbin@schellmanco.com), matt.crane@schellmanco.com, and 3 more  
01/15/2018 - 9:57:24 AM PST