MDRP New Service Provider Management Checklist

Service Provider:_____Date:_____

MDRP Name: _____ MDRP Signature of Approval_____

****Please note: the MDRP is responsible for managing the Service Provider(s) utilized in their department.**

Proposed Service Providers with a payment card component (this includes vendors processing payment card data on Middlebury's behalf), or that can impact the security of payment card data, must provide the following documentation to the PCI Compliance Team, and meet the below requirements, to be considered a Service Provider for Middlebury:

_____ Written contract/agreement with Service Provider must include the Data Privacy and Breach Notification language and a minimum liability insurance coverage- must be signed by Service Provider.

_____ **eCommerce solutions (includes online storefront):**

- _____ Encryption protocol must be TLS 1.1 or greater. TLS 1.2 is preferred, SSL and TLS 1.0 are no longer considered secure or compliant.
- _____ Provide either an SAQ D-Service Provider Attestation of Compliance (AOC) or an On-Site Assessment AOC for Service Providers. Any other SAQ is not applicable. The AOC must be for the Service Provider we are contracting with, the Service Provider cannot rely on third party service provider's compliance. PCI Compliance Validation Date:_____
- _____ The AOC must specifically note assessment of the service being provided.
- _____ Provide a recent quarterly vulnerability scan by their ASV.
- _____ Have the proposed Service Provider complete the http://go.middlebury.edu/saas Security Survey. Let the PCI Team know Service Provider has completed.
- _____ Submit a card flow diagram, also known as a data flow diagram, noting all third party Service Providers involved in the process.
- _____ Matrix of PCI Responsibilities Service Provider is responsible for- This is part 2G of the AOC.

_____ **Card present solutions:**

_____ Must be listed on the Payment Card Industry Security Standards Council (PCI SSC) validated Point to Point Encryption (P2PE) solution. Service Provider must provide the PCI SSC Validation number. Enter the PCI SSC Validation Number _____.

_____ If a **non-P2PE** Payment Application is being considered, it must be listed on the PA DSS Validated Application List. PA DSS Validation number: _____.

NOTE- NON-P2PE VALIDATED SOLUTIONS ARE SUBJECT TO ADDITIONAL REQUIREMENTS AND SIGNIFICANT COST TO THE MERCHANT DEPARTMENT.

_____ **Point of Sale solutions**: Must use only Payment Card Industry (PCI)-certified Qualified Integrators and

Reseller (QIR) professionals for point-of-sale (POS) application and terminal Installation and integration. Name of QIR: _____

_____ Encryption protocol must be TLS 1.1 or greater. TLS 1.2 is preferred, SSL and TLS 1.0 are no longer considered secure or compliant.

_____ Provide either an SAQ D-Service Provider Attestation of Compliance (AOC) or an On-Site Assessment AOC for Service Providers. Any other SAQ is not applicable. The AOC must be for the Service Provider we are contracting with, the Service Provider cannot rely on third party service provider's compliance.

_____ The AOC must specifically note assessment of the service being provided.

_____ Provide a recent quarterly vulnerability scan by their ASV.

_____ Have the proposed Service Provider complete the http://go.middlebury.edu/saas Security Survey. Let PCI know Service Provider has completed.

_____ Submit a card flow diagram, also known as a data flow diagram, noting all third party Service Providers involved in the process.

_____ Matrix of PCI Responsibilities Service Provider is responsible for- This is part 2G of the AOC.

A current and comprehensive list of Service Providers must be maintained by Middlebury. MDRP's must keep a list of Service Providers they are responsible for managing. The comprehensive list is located at Service Provider Matrix and AOC Tracker and will be maintained by the PCI Compliance team.

***Note:** All Service Providers must complete **either** an Self Assessment Questionnaire (SAQ) D-Service Provider AOC or an On-Site Assessment AOC for Service Providers. Any other SAQ is not applicable to a Service Provider.

AOC Attestation of Compliance
SAQ Self Assessment Questionnaire