PCI- DSS Requirement 12.8

Management of Service Providers Policy and Procedures

12.8 Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, (Department X) has established a formal policy and supporting procedures concerning management of service providers. This policy will be evaluated on an annual basis to ensure adequacy and relevancy regarding (DEPATEMENT X'S) needs and goals. During this review process, a new Attestation of Compliance (AOC) and Visa Global Registry check will be performed for the vendor to validate ongoing compliance with PCI OSS.

Document Creation	XX/XX/2017
Document Signed	XX/XX/2017

Review Date	Reviewed By

12.8 Policy

DEPARTMENT X will ensure that the Management of Service Providers policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Current Version – presently 3.2):

- A current and accurate list of service providers is to be maintained, complete with contact information of all personnel.
- For any services engaged with service providers that may affect or have a relationship or function associated with DEPARTMENT'S cardholder data environment, the written agreement shall include an acknowledgement by the service providers of their responsibility for securing cardholder data.
- Due diligence must be exercised before engaging with any service providers that may affect or have a relationship or function associated with DEPARTMENT'S cardholder data environment.
- Maintain a program to monitor service providers' PCI DSS compliance status at least annually. This is performed by obtaining an Attestation of Compliance (AOC) report from the service provider.
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

12.8 Procedure

DEPARTMENT X has developed and implemented a comprehensive Management of Service Providers program, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by DEPARTMENT X – NAMED POSITION to ensure that the management of service provider's initiatives are executed in a formal manner and on a consistent basis.

TABLE 12.8

LIST OF SERVICE PROVIDERS

Name of Service Provider	Primary Function	Name and Contact Information of Service Provider Personnel	Due Diligence Conducted on Service Provider	Contractual Documentation and Written Agreements in Place	Program Used for Monitoring Service Provider Compliance
Vendor X	Processor		Visa Global Registry	Y	Yearly AOC

Requirement Which Agency is Responsible For	Requirement Which Vendor is Responsible For
Verify vendor maintains PCI compliance on a yearly basis through AOC and Visa Global Registry	Remove sensitive authentication data and limit data retention
Coordinated Incident/data breach response with vendor	Protect systems and networks, and be prepared to respond to a system breach
	Secure payment card applications
	Monitor and control access to your systems
	Protect stored cardholder data
	Finalize remaining compliance efforts and ensure all controls are in place
	Report suspected compromise of cardholder data to Department Management and merchant service bank and follow their procedures for investigation

12.8 Responsibilityfor Policy Maintenance

The (Named Department Contact) is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

Position name	Date