

# Managing Service Providers Procedure

Reference: PCI POL 12.2

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 29/06/2020

Organisation Issue Date:

## 1. Scope

Organisation Name shares cardholder data with

"service providers for back-up/storage facilities, managed service providers such as web/cloud hosting companies or security service providers, or those that receive data for fraud modelling purposes."

Any external parties with whom Organisation Name shares cardholder data are subject to this procedure.

## 2. Responsibilities

### 2.1 All

"Relationship Owners"

who are responsible for services provided by third-party service providers are required to ensure that external parties have entered into a formal service provider agreement under this procedure, which acknowledges that the service provider is responsible for the security of cardholder data the service provider possesses.

### 2.2

"Relationship Owners"

are responsible for ensuring that service providers comply with PCI DSS and that this compliance status is monitored at least annually.

2.3 The Information Security Manager maintains a list of service providers (List of Service Providers) with whom Organisation Name has approved contracts. A record of the agreements and date(s) on which the service providers are required to revalidate their PCI compliance, must be maintained. The list (Shared Responsibility Matrix) identifies the services provided, the extent to which the service provider and any of their service providers are responsible for the security of cardholder data, but is superseded by the Attestation of Compliance (AoC) should one be present.

### 3. Procedure

3.1 Where there is a business need for working with a service provider, Organisation Name ensures that its cardholder data security is not reduced; service providers are required to comply with PCI DSS, completing and providing Organisation Name with a copy of the current AoC – Service Providers.

3.2 Clearly identify the services and system components that are included in the scope of the service provider's PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements that are the responsibility of the service provider's customers to include in their own PCI DSS reviews. This will all be detailed within the service provider's AoC which is used as the ultimate authority of the service providers capability.

3.3 Organisation Name carries out due diligence to identify risks related to external party access.

3.4 The due diligence process identifies and documents, for each service provider:

- The corporate status of the service provider, including its registered address and related information.
- The financial status of the service provider, by means of a credit status check.
- The performance of the service provider, by means of at least two written references from existing customers.
- The quality and security practices of the service provider, by checking the validity of its current certificates to ISO/IEC 27001 (information security), ISO 9001 (quality management) and ISO/IEC 20000 (IT service management).
- Details of court cases, complaints and any other issues that might be addressed by an extensive Google search.

"3.5 Enter additional steps/details as required"

### ***Document Owner and Approval***

The Information Security Manager is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).

SAMPLE