<COMPANY>

P07 - Third Parties Policy

Document Reference	P07 - Third Parties Policy
Date	8th October 2014
Document Status	Final
Version	3.0
Revision History	1.0 9 November 2009: Initial release. 1.1 17 November 2009: Procedural updates. 1.2 08 January 2010: Update to reflect December changes. 2.0 03 January 2012: Update to reflect PCI DSS v2.0 changes. 3.0 October 2014: Update to reflect PCI DSS v3.0 changes.

Table of Contents

1. Policy Statement

This document details **<COMPANY>'s** policy in relation to Service Providers and Third Parties that store, process or transmit **<COMPANY>'s** payment card data.

Detailed below are the PCI compliance tasks, security standards and procedures required of these Service Providers and third parties.

- This document should be viewed in conjunction with **<COMPANY>'s** top-level security policy: P01 – Information Security Policy.

2. Review and Update of the Policy Statement

The Policy Statement and associated company Policies are reviewed at least annually by **<COMPANY>'s [RESPONSIBLE TEAM]** to ensure:

- The business meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS).
- It maintains its relevance to the business' current and planned payment card processing operations.

The **<COMPANY>'s [RESPONSIBLE TEAM]** will undertake the technical review of this policy statement and associated company Policies.

3. Purpose

This document details what is expected of each Service Provider and Third Party when storing, processing or transmitting **<COMPANY>'s** payment card data.

It is very important that each identified external organisation that has access to card data exercises a duty of care. In certain cases, such as with Payment Gateways, Payment Processors, Hosting Providers and Third Party Application Providers, proof of PCI compliance must be provided. This information will feed directly into **<COMPANY>'s** PCI compliance programme.

Service Providers and Third Parties are listed in document: F20 - Service Providers Log.

4. Scope

This document provides instruction on dealing with external companies that have access to **<COMPANY>'s** payment card data or payment card processing facilities.

It is restricted to those companies or contractors that process, store or transmit card data on behalf of **<COMPANY>**, or have access to such systems.

5. External Company Definitions

It is important to distinguish between Service Providers and Third Parties.

Once Service Providers have been identified, supporting PCI audit materials shall be requested as proof of compliance. Proof of compliance ensures that the Service Provider is meeting its security obligations when handling card data on behalf of **<COMPANY>**. **<COMPANY>** shall ensure that each Service Provider's continued PCI DSS compliance status is confirmed at least annually.

5.1. Service Providers

An entity that stores, processes or transmits cardholder data on behalf of another organisation, or has access to another organisation's CDE.

This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data.

Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications

companies that only provide communication links without access to the application layer of the communication link are excluded.

<COMPANY> must:

- Maintain a list of service providers.
- Maintain a written agreement with each service provider that includes an acknowledgement by the service provider that they are responsible for the security of cardholder data they possess or otherwise store, process or transmit on behalf of <COMPANY>, or to the extent that they could impact the security of the client's cardholder data environment.
- If <COMPANY> is *also* acting as a service provider, then <COMPANY> must provide a written agreement to clients as per the point above, in order for clients to maintain their own PCI compliance.

Service Providers are categorised by the nature of card processing activity and / or the number of card transactions that they process on behalf of their clients. There are two levels as mandated by the Card Schemes (Visa, Mastercard, Amex et al):

Service Provider Level	Description
1	Any service provider that stores, processes, or transmits more than 300,000 card transactions annually.
2	Any service provider that stores, processes, or transmits fewer than 300,000 card transactions annually.

5.2. Service Providers Providing Card Processing Software or Services

Third parties providing card data processing systems such as payment gateways, PED terminals or payment processing software are required to do so in accordance with the relevant PCI standard.

See Section 6.1 below.

6. Policy

6.1. General

As part of **<COMPANY>'s** continuing obligation to PCI DSS compliance, due diligence checks, such as:

- Confirmation of PCI compliance status, including which specific PCI DSS requirements are being met or supported by the service being offered (this may include details of the provider's PCI DSS compliance, PA DSS compliance, PTS compliance, or P2PE compliance, as applicable)
- **<COMPANY** to define>**,**
- **<COMPANY** to define>**,**

are conducted before:

- Selecting and implementing a new Service Provider.
- Connecting any external company to the card processing network.

- Granting external organisations access or control over **<COMPANY>'s** card data.
- Selecting and deploying payment card processing software or services within the organisation.

Note that the PCI compliance status of all service providers, and the corresponding PCI DSS requirements that are being met or supported by the provider needs to be reconfirmed and documented annually.

A full list of service providers and third parties accessing card networks can be found in the document: F20 - Service Providers Log.

6.2. Agency Background Checks

<COMPANY> shall ensure that any and all agencies providing staff on a temporary basis have conducted background checks against the staff being provided, including:

- Reference Checks.
- Employment History Checks.
- Immigration Status & Right to Work checks.

<COMPANY> shall maintain a list of the Agencies used, and the checks performed by each agency:

A full list of Agencies used by the **<COMPANY>** can be found in the document: F20 - Service Providers Log.

7. Glossary and References

7.1. Glossary

- **See document "P99 - Glossary"**

7.2. References

- P01 - Information Security Policy
- F20 - Service Providers Log