<COMPANY>

P01 - Information Security Policy

Document Reference	P01 - Information Security Policy
Date	30th September 2014
Document Status	Final
Version	3.0
Revision History	1.0 09 November 2009: Initial release. 1.1 17 November 2009: Procedural updates. 1.2 22 December 2009: Updated Styles. 1.3 14 September 2010: Update Policy Pack review changes. 1.4 18 January 2011: Mechanism of IS Policy distribution. 2.0 03 January 2012: Update to reflect PCI DSS v2.0 changes. 3.0 September 2014: Update to reflect PCI DSS v3.0 changes.

Table of Contents

1. Policy Statement 3
2. Review and Update of the Policy Statement 3
3. Purpose 3
4. Scope 3
5. Information Security Framework 4
5.1. Reporting Structure for the Business 4
5.2. Associated Teams 4
5.3. Annual Policy Review 4
5.4. Policy Breaches 5
5.5. Individual Policies 5
5.6. Policy Communication 6
5.6.1. Policy Creation and Distribution 6
5.6.2. Security Training 6
5.6.3. Employment Checks 7
5.6.4. Data Confidentiality for Service Providers / Third Parties 7
6. Glossary and References 8
6.1. Glossary 8
6.2. References 8

1. Policy Statement

This **<COMPANY>** Information Security Policy Statement ("Policy Statement"):

- Sets out **<COMPANY>'s** high level requirements for the management of Information Security across **<COMPANY>** in relation to the storage, processing and transmission of payment card data.
- Defines the Information Security Policy Statement for the business.
- Applies to all Payment card Processing operations for the business.

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.

Any changes this policy will be communicated to all members of **<COMPANY>'s [RESPONSIBLE TEAM]** and any other stakeholders (which may include vendors and business partners).

3. Purpose

This document details the security strategy for **<COMPANY>** in relation to the storage, processing and transmission of payment card data. Its aim is to provide a detailed understanding of Information Security responsibilities for all levels of staff, contractors, partners and third parties that access **<COMPANY>'s** Card Data Environment (CDE).

As part of **<COMPANY>'s** Payment Card Industry (PCI) Compliance programme, consideration has been made to Payment card Processing operations. Guidelines and controls form an essential part of the company's compliance status against the PCI Data Security Standard.

4. Scope

This document must be reviewed by parties involved with **<COMPANY>'s** payment card processing operations. Specifically:

- Day-to-day payment card processing operations (including IT systems).
- Implementation of new payment card processing systems.
- Maintenance of existing payment card processing.

This document should also be used for reference purposes when **<COMPANY>** undertakes its annual PCI compliance review.

The policy framework maps directly to the PCI DSS and that information can be found in F16 - Standards Matrix.

5. Information Security Framework

5.1. Reporting Structure for the Business

Within **<COMPANY>**, **<COMPANY> to update** is responsible for matters relating to Information Security and is designated the Head of Information Security.

Name	Title / Description	Contact Details
<COMPANY> to update	**<COMPANY> to update**	**<COMPANY> to update**

This role/ These roles has/have responsibility for:

- Overall responsibility for Information Security and related issues.
- Development and maintenance of Information Security Policies and Procedures (including distribution to; and training of, staff in policies).
- Communication and review of Information Security Policies.
- Coordination of PCI Security Audit Tasks.
- Coordination with PCI Accredited Security Auditors (QSAs and ASVs).
- Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel
- Establishing, documenting, and distributing security incident response and escalation procedures
- Keeping IT security staff and management updated on all security related issues.

5.2. Associated Teams

The following teams are directly involved in **<COMPANY>'s** PCI compliance programme. References to these teams are made throughout **<COMPANY>'s** suite of PCI policies.

Team Name	Functions (with respect to PCI)	Team Contact Details
PCI review team	**<COMPANY> to update**	**<COMPANY> to update**
IT Systems Team	**<COMPANY> to update**	**<COMPANY> to update**
Development Team	**<COMPANY> to update**	**<COMPANY> to update**
Change Control Team	**<COMPANY> to update**	**<COMPANY> to update**
Internal Audit Team	**<COMPANY> to update**	**<COMPANY> to update**

5.3. Annual Policy Review

All Information Security Policies are reviewed and where necessary updated on at least an annual basis, or upon significant change to the CDE (whichever happens first).

The review process ensures that:

- Policies in place are still required.
- Perceived threats facing **<COMPANY>** are identified and consideration included in procedural documentation.
- Any new legal issues are identified that require changes in current policy or practice.
- **<COMPANY>** meets current PCI compliance standards.

- Any changes to network configuration or new applications are included in **<COMPANY>'s** security policy.

A formal documented risk assessment process must also be completed annually to identify key business assets (including the CDE, payment card data stores and supporting networks), and potential threats and vulnerabilities which could impact on the security of those assets.

5.4. Policy Breaches

Company disciplinary procedures will be invoked in the case of staff or third parties breaching the Policy Statement and /or any supporting policies or standards.

5.5. Individual Policies

The policies listed below have been developed in accordance with the current version of the PCI Data Security Standard. This is currently: Version 3.0

Policies address all requirements listed in the Data Security Standard.

Specific policies are listed below:

Policy Name	**Document Name**
Information Security Policy	P01 - Information Security Policy
Audit Policy	P02 - Audit Policy
Disaster Recovery & Security Incident Response Policy	P03 - Disaster Recovery & Security Incident Response Policy
Wireless Access Policy	P04 - Wireless Access Policy
Operational Policy	P05 - Operational Policy
Acceptable Use Policy	P06 - Acceptable Use Policy
Third Parties Policy	P07 - Third Parties Policy
Information Classification Policy	P08 - Information Classification Policy

Policy Name	Document Name
Key Management Policy	P09 - Key Management Policy
Physical Security Policy	P10 - Physical Security Policy
Systems and Application Development Policy.	P11 - Systems & Application Development Policy

5.6. Policy Communication

5.6.1. Policy Creation and Distribution

The **<COMPANY> [ROLE NAME]** has overall responsibility for the creation and distribution of IT Security Policies and Procedures (**<COMPANY>** to document how the information security policy is distributed for viewing by all employees and third parties who are authorised to access cardholder data).

All staff are reminded that the policy and related documents are sensitive and must not be removed from **<COMPANY>'s** premises or networks.

5.6.2. Security Training

All changes and additions to policy are circulated to stakeholders at least one (1) day in advance to allow time for them to adapt to changes. **<COMPANY>** does however reserve the right to modify policy immediately and without prior notice.

Staff are kept aware of policies via the following (**<COMPANY> to define**) methods of communication:

- Staff meetings.
- Emails, Intranet or Staff Bulletins.
- Posters.
- Mock exercises.

Data security awareness training, including authentication procedures and policies, and (for POS environments) awareness of the risk of Pin Entry Device tampering, is to be conducted for new starters during induction, and for all staff, at least annually to make all personnel aware of the importance of cardholder data security. The training will address the following specific areas as a minimum:

- Guidance on selecting strong authentication credentials.
- Guidance for how users should protect their authentication credentials, and why sharing passwords is a poor security choice.
- Why it is important not to reuse previously used passwords.
- How to change passwords if there is any suspicion the password could be compromised.

- Training personnel to be aware of suspicious behaviour and to report tampering or substitution of POS devices to <RESPONSIBLE TEAM>.

<COMPANY> shall also ensure that vendors, contractors, and business partners covered by this policy are familiar with these requirements.

Once a new policy has been introduced, following significant changes, and at least annually, all staff must endorse the IT security policies. This ensures that they have read and understood the policy (or changes) and accept any consequences should they fail to adhere to them.

Users will be made familiar with the password procedures for **<COMPANY>** and will be offered specialist training if necessary.

Staff with cardholder data access:

Staff with privileged access, deemed to have the *need to know* (see PCI DSS Requirement 7) must be given extra training to ensure they are aware of the significance of the data being held and the repercussions of disclosing it to those who do not have the *need to know*.

Staff Acknowledgement

Staff are required to acknowledge (in writing, or electronically) that they have attended any security awareness courses, and a log must be maintained to that effect.

5.6.3. Employment Checks

<COMPANY> shall ensure that any new employee directly hired by the company shall be subjected to the following checks, where the employee will have access to cardholder data or the cardholder data environment. (**<COMPANY> to define)**:

- Reference Checks.
- Previous Employment History Checks.
- Right to Work status.
- Criminal record checks.
- Credit history checks.

<COMPANY> shall ensure that any agency providing temporary staff at any point within the year shall ensure that the agency contracted, to provide such staff, has conducted the above checks and can produce the relevant documentation upon request (see also P07 - Third Parties Policy).

All information gathered for employment checks shall be maintained in the employee's personnel file.

5.6.4. Data Confidentiality for Service Providers / Third Parties

<COMPANY> has a duty of care to its customers and a PCI Compliance obligation to ensure that Service Provider and Third Parties processing or given access to sensitive card data uphold suitable Data and Information Security Practices and Policies.

PCI Compliance for Service Providers follows the PCI DSS. For more information on Service Providers and Third Parties with access & processing responsibility for card holder data see P07 - Third Parties Policy.

6. Glossary and References

6.1. Glossary

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

6.2. References

- P01 - Information Security Policy
- P02 - Audit Policy
- P03 - Disaster Recovery & Security Incident Response Policy
- P04 - Wireless Access Policy
- P05 - Operational Policy
- P06 - Acceptable Use Policy
- P07 - Third Parties Policy
- P08 - Information Classification Policy
- P09 - Key Management Policy
- P10 - Physical Security Policy
- P11 - Systems & Application Development Policy
- F16 - Standards Matrix