

<COMPANY>

P01 - Information Security Policy

Document Reference	P01 - Information Security Policy
Date	
Document Status	SAMPLE
Version	2.0
Revision History	

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	3
5.1.	Reporting Structure for the Business	3
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	6
5.6.4.	Data Confidentiality for Service Providers / Third Parties	7
6.	Definitions and References	7
6.1.	Definitions	7
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 credit card data.
- Defines the Information Security Policy Statement for the business.
- Applies to all Credit 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 credit 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 the security strategy for <COMPANY> in relation to the storage, processing and transmission of credit 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 credit card processing network.

As part of <COMPANY>'s Payment Card Industry (PCI) Compliance programme, consideration has been made to Credit 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 should be reviewed by parties involved with <COMPANY>'s credit card processing operations. Specifically:

- Day-to-day credit card processing operations (including IT systems).
- Implementation of new credit card processing systems.
- Maintenance of existing credit 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 has 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 (QSA's and ASV's).
- Overall monitoring and analysis of security alerts, and distribution to appropriate <COMPANY> personnel..
- 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
<i>PCI review team</i>	<COMPANY> to update	<COMPANY> to update
<i>IT Systems Team</i>	<COMPANY> to update	<COMPANY> to update
<i>Development Team</i>	<COMPANY> to update	<COMPANY> to update
<i>Change Control Team</i>	<COMPANY> to update	<COMPANY> to update
<i>Internal Audit Team</i>	<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.

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 should also be completed annually to identify key business assets (including credit 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 2.0 - dated October 2010.

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
Key Management Policy	P09 - Key Management Policy
Physical Security Policy	P10 - Physical Security Policy

Policy Name	Document Name
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 documents are sensitive and should not be removed from <COMPANY>'s buildings / offices.

5.6.2. Security Training

Changes to, removal of, or the introduction of policies are circulated to relevant parties 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 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, 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.

<COMPANY> shall also ensure that vendors, contractors, and business partners covered by this policy are familiar with its 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) should 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*.

5.6.3. Employment Checks

<COMPANY> shall ensure that any new employee directly hired by the company shall be subjected to the following checks (<COMPANY> to define):

- Reference Checks.

- Previous Employment History Checks.
- Immigration Status and 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. Definitions and References

6.1. Definitions

- **IS:** Information Security
- **Payment Card Industry Data Security Standard (PCI DSS):** Currently referenced directly from The PCI Security Standards Council's online resource at <https://www.pcisecuritystandards.org>
- **QSA:** Qualified Security Assessor. A third party assessor that conducts onsite PCI audits for Service Providers and Merchants. The QSA is certified annually by The PCI Security Standards Council.
- **ASV:** Approved Scanning Vendor. A third party assessor that conducts quarterly PCI scans against the external card processing environment. The ASV is certified annually by The PCI Security Standards Council.
- **Schemes.** Credit Card Associated companies that include Visa, MasterCard, Amex, JCB, Diners.
- **Merchant.** For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and / or services. Note that a merchant that accepts payment cards as payment for goods and / or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
- **Service Provider.** Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. 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.

- **Acquirer.** Bankcard association member that initiates and maintains relationships with merchants that accept payment cards.
- **Cardholder data:** Full magnetic stripe or the PAN plus any of the following: Cardholder name, Expiration date, Service Code.
- **Cardholder Data Environment:** Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

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