

# The Payment Card Industry Data Security Standard

## PCI DSS COMPLIANCY

### What is PCI DSS?

PCI DSS (Payment Card Industry Data Security Standard) is essentially a comprehensive framework of security controls aimed at protecting card payment data. It is a global standard developed by the major card schemes, governed and maintained by the PCI Security Standards Council and enforced on merchants by their acquiring banks.

The official deadline imposed on the UK was June 2006 so organisations that aren't compliant need to start demonstrating a clear plan to achieve compliance. The objective of the standard is to reduce the risk to card holders from the threat of identity theft, fraud and financial loss.

As a "Data" security standard it is not surprising to learn that it is fundamentally technical in nature, focussing on specific IT security controls for **all** systems that store, transmit or process payment card data. There are, however, several business-level controls which are also covered, focusing on policy, awareness and process; all must be considered. All merchants need to certify that they comply with the standard and while the assessment approach may differ depending on your acquiring bank, the actual need to address all controls in the standard is applicable to all merchants.

Organisations that fail to meet the compliance requirements are at risk of higher card transaction rates or even losing their ability to process payment cards altogether. They are also unlikely to understand the security risks that put their customers' data and the organisation's own reputation and share value in jeopardy. Furthermore, organisations that suffer a compromise to card holder data are subject to potentially large financial losses as a result of forensic investigations, card re-issue costs being passed on from the bank and lost business.



### Pasporte's Approach to PCI DSS Compliancy

Pasporte InfoSec & Compliance Specialists have years of experience helping a broad range of organisations address their IT and business security and related compliance issues. Our people typically hold CISSP (Certified Information System Security Professional), CISM (Certified Information Security Manager) and ISO 27001 Lead Auditor qualifications and are members of the Institute of Information Security Professionals. We offer bespoke services aimed at taking the pain out of managing security risks and meeting industry regulation; we specialise in implementing InfoSec improvement and compliance strategies; developing secure IT and business processes; and architecting secure IT infrastructure.

We adopt proven methodologies covering areas such as policy development and implementation, awareness education, security testing, risk assessment, system architecture management and system hardening.

Furthermore, Pasporte's secure hosting service provide retailers with a ready-made springboard to compliance, enabling the rapid deployment of mandatory services such as log management, charge detection and vulnerability scanning.

Pasporte takes a three staged approach to PCI compliancy

1. **PCI Scoping & Gap Analysis**
2. **PCI Compliance Programme Management**
3. **PCI Security Management**

**Contact Toby Walton today on 01276 450412 to take advantage of special discounted rates for May! enquiries@pasporte.com**