

PCI Data Security Systems (PCI DSS), PCI Pin Transaction Security (PCI PTS) and our Clients



What is PCI DSS

Payment Card Industry Data Security Standard (PCI DSS v1.2) is a global data security standard adopted by the Payment Card Industry Security Standards Council for all organisations that process, store or transmit cardholder data. PCI DSS consists of a standardised, industry-wide set of requirements and processes for security management, policies, procedures, network architecture, software design and critical protective measures. This would include, but is not limited to acquiring banks, merchants and third parties. Paper and electronic information is required to be appropriately stored, transmitted and used. This includes the following: card numbers, expiry dates, PIN, CVV numbers and details used in online transactions such as passwords, email address and names.

What are the benefits of compliance

Protection of customer data, increased customer confidence and aiding in the safeguarding of the reputation of brands as well as helping to ensure best practice.

Compliance & Auditing

PCI DSS compliance consists of several steps that mirror best security practices. Meeting PCI program compliance requirements is critical as card issuer (Visa, MasterCard, American Express etc.) can levy penalties on merchant or service providers who are not in compliance. This document will not detail all measures for compliance and the process for auditing compliance. A brief checklist for PCI DSS requirements is included at the end of this document, and provides an overview of compliance requirements.

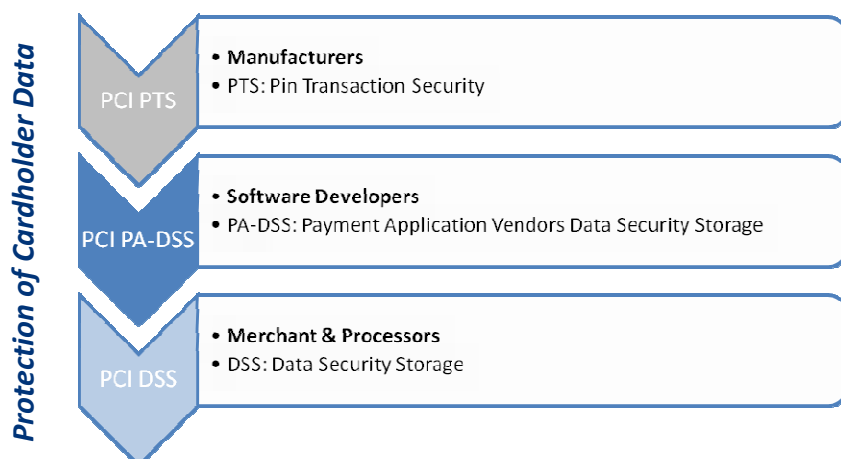
More information is available from <https://www.pcisecuritystandards.org>

EPOSability Ltd and PCI DSS Compliance

Although EPOSability Ltd do not actually process, store, have access or transmit any cardholder data from our clients. We do recognize a duty of due diligence to ensure that the equipment we provide and maintain for our clients will aid in their PCI DSS compliance. This involves ensuring compliance with Payment Card Industry Pin Transaction Security (PCI PTS).

PCI PTS is a set of security requirements focused on the characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The PCI Security Council has set out requirements for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it. EPOSability Ltd ensures as part of our procurement process that our clients only use devices or components that are tested and approved by the PCI SSC, and complies with the requirements of PCI PTS. EPOSability Ltd will ensure that all existing equipment and all new equipment maintained and provided by EPOSability Ltd (at its point of installation) is PCI PTS compliant.

Payment Card Industry Security Standards



Payment Card Industry Data Security Standard (PCI DSS) EPOSability Ltd and PCI DSS (Continued)



Figure 1: PCI DSS Framework Requirements (An Overview)

Goals	PCI DSS Requirements
Building and Maintaining a Secure Network	1.] Install and maintain a firewall configuration to protect cardholder data 2.] Do not use vendor supplied defaults for passwords and other security parameters
Protect Cardholder Data through your infrastructure	3.] Protect stored cardholder data 4.] Encrypt transmission of cardholder data across open, public networks.
Maintaining an effective Vulnerability Management Programme	5.] Use and regularly update anti-virus software or programs 6.] Develop and maintain secure systems and applications
Implement effective and strong Access Control Measures	7.] Restrict access to cardholder data by business need-to-know 8.] Assign a unique ID to each person with computer access 9.] Restrict physical access to cardholder data
Regularly Monitor and Testing of Networks	10.] Track and monitor all access to network resources and cardholder data 11.] Regularly test security systems and processes
Maintaining an Information Security policy that addresses Information Security Requirements	12.] Maintain a policy that addresses information security for employees and contractors.

EPOSability