Computer Security Solutions

Retailers Guide to PCI DSS

WHAT IS PCI DSS?

PCI DSS stands for **Payment Card Industry Data Security Standard**. The standard was established under the administration of an independent body, The PCI Security Standards Council (PCI SSC).

PCI DSS consists of standardised, industry wide set of requirements and processes. Its purpose is to ensure that valuable credit/debit card data is always secure.

PCI DSS was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc during 2004. Until this point the credit card companies had operated individual data security programs but determined that if they are to effectively tackle credit card fraud, hacking and other security incidents they need to join forces and create one source of governance, enforcement and knowledge.

PCI DSS stands for **Payment Card Industry Data Security Standard**. The standard is established under the administration of an independent body the PCI Security Standards Council (PCI SSC).

DOES MY BUSINESS NEED TO COMPLY WITH PCI DSS?

In general **all** businesses that accept or processes credit and debit cards, whether the transaction takes place over the phone, via the internet (including another company doing so on your behalf) or via Chip and PIN, must comply with the PCI DSS data standards.

If you are still unsure if this standard applies to your particular business it recommended to you contact your bank or service provider in the first instance.

All businesses that accept or processes credit and debit cards, must comply with the PCI DSS data standards.

HOW IS IT GOING TO WORK IN PRACTICE?

PCI DSS is a relatively new standard that business has to come to terms with. It is envisaged that businesses will receive notification from their bank or service provider regarding becoming compliant. It is probable that each provider will have its own compliance programme.

Before contacting a consultant or assessor for advice, read your providers criteria carefully. If you have questions discuss them with the provider first.

WHAT IF I DO NOTHING?

It is the banks and not the brands or the PCI SSC who will enforce compliance with this standard.

If businesses fail to gain compliance with this standard it will be the business who will incur the costs of being compromised and used fraudulently and not the payment card companies or the banks.

A company processing storing or transmitting payment card data must be PCI compliant or risk losing their ability to process card payments and or be fined.

If a business is not compliant and is the victim of compromise the business and not the payment card company will incur costs.

HOW DO I ACHIVE PCI DSS COMPLIANCE?

Firstly assess which level of business you are and your requirements.

If are unsure which level applies to your business it would be worthwhile contacting your bank or service provider.

For Merchants		
	Criteria	**Compliance Requirements**
Level 1	More than 6 million transactions annually	Annual on-site audit by a QSA Quarterly network security scan
Level 2	1,000,000 - 5,999,999 transactions annually	Annual self assessment questionnaire Quarterly network security scan
Level 3	20,000 to 1 million e-commerce transactions annually	Annual self assessment questionnaire Quarterly network security scan
Level 4	Up to 20,000 e-commerce transactions only	Annual self assessment questionnaire Quarterly network security scan

LEVEL 1 BUSINESS REQUIREMENTS

The requirements are:

a. An annual on-site security audit carried by a Qualified Security Assessor (QSA). To view the current list of QSAs recognised by PCI Security Standards Council visit:

https://www.pcisecuritystandards.org

b. A quarterly network security scan by an Approved Scanning Vendor (ASV).

The QSA will contact each payment card company to determine each company's reporting requirements and instructions and present a report on their findings.

LEVEL 2 - 4 BUSINESS REQUIREMENTS

Level 2 - 4 Businesses must complete a Self-Assessment Questionnaire (SAQ). There are four types of questionnaires. Which one you complete depends on the way you conduct your business and accept payment.

Use the table below to gauge which SAQ applies to your organisation. By visiting https://www.pcisecuritystandards.org you can review the detailed descriptions contained within each document to ensure you meet all the requirements for that SAQ.

SAQ Validation Type	Description	SAQ
1	Card-not-present (e-commerce or mail/telephone-order) business, all cardholder data functions outsourced. This would never apply to face-to-face business. **Details**: Business does not store, process, or transmit any cardholder data on business premises but relies entirely on third party service provider(s) to handle these functions. Business does not store any cardholder data in electronic format; **and** If business does store card holder data, such data is only in paper reports or copies of receipts and is not received electronically.	**A**
2	Imprint-only business with no electronic cardholder data storage. **Details**: Business uses only imprint machine to imprint customers' payment card information and does not transmit card holder data over either a phone line or internet . Business does not store card holder data in electronic format; **and** If Business does store cardholder data, and such data is only paper reports or copies of paper receipts and is not received electronically.	**B**
3	Stand-alone terminal business, no electronic cardholder data storage.	**B**

	Details: Business uses only standalone dial up terminals and the standalone dial up terminals are not connected to the internet or any other systems within the business environment. Business does not store card holder data in electronic format:; **and** If Business does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.	
4	Business with Point of Sale systems (Chip & PIN etc) connected to the Internet, no electronic cardholder data storage. **Details**: Business has a payment application system and an internet or public network connection on the same device; The payment application system/internet device is not connected to any other system within the business environment; If Business does not store cardholder data in electronic format; Business does store any cardholder data in electronic format; **and** If business does store card holder data, such data is only in paper reports or copies of receipts and is not received electronically; **and** Business's payment application software vendor uses secure techniques to provide remote support to business's payment application system.	**C**
5	All other businesses (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete a SAQ.	**D**

If you are unsure which level applies to your business it is recommended that you contact your bank or service provider.

ANNUAL SELF-ASSESSMENT QUESTIONNAIRE

The Self-Assessment Questionnaire is a free tool that can be used to gauge the business's level of compliance with PCI DSS.

Businesses may wish to complete the Self-Assessment Questionnaire themselves, however, they can obtain the services of a security professional if they wish (a QSA is **not** required).

The Self-Assessment Questionnaire is a series of 'yes'/'no' questions relating to the PCI DSS requirements.

The Self-Assessment Questionnaire is a series of yes/no questions relating to PCI DSS requirements

Depending on which SAQ is completed you will be required to demonstrate that your business meets some or all the following requirements. The requirements for your level of business are laid out within the SAQ.

SAQ A - Confirm business practices comply with DSS Requirements 9 & 12.

SAQ B - Confirm business practices comply with DSS Requirements 3, 4, 7, 9, 12.

SAQ C - Confirm business practices comply with all the DSS Requirements with the exception of Requirement 10.

SAQ D - Confirm business practices comply with all the DSS Requirements.

WHAT ARE THE PCI DSS REQUIREMENTS?

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organised:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmissions of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

QUATERLY NETWORK SCANS

Quarterly network scans are referred to as vulnerability scans and they ensure that a business's systems are protected from external threats (such as hacking or malicious viruses). The scanning tools test all of their network equipment, hosts, and applications for known vulnerabilities.

Scans are intended to be non-intrusive, and are conducted by an authorised network security scanning vendor.

Regular scans are necessary to ensure that the businesses systems and applications continue to afford adequate levels of protection. If the scans identify any vulnerabilities a follow-up scan will be necessary to ensure that the remediation was successful.

CHIP AND PIN DEVICES

PIN Entry Devices (PED) must also comply with the PCI DSS security requirements. Check your PED terminals and software applications to ensure they have passed PCI compliance validation. If your device or software is not listed or you are still unsure contact your bank or service provider.

In order to comply with PCI DSS, business will need to provide positive answers to each of the questions or to indicate (where this is a valid option) that they do not apply to their business.

PCI DSS COMPLETED

Once the SAQ has been completed, the business will be able to make a good assessment of their risk exposure.

In order to comply with PCI DSS, businesses will need to provide positive answers to each of the questions or to indicate (where this is a valid option) that they do not apply to their business.

Regular reports are required for PCI compliance; these are submitted to your the requesting bank or card payment brand that you do business with.

PCI SSC is not responsible for PCI compliance. All businesses and processors must submit a quarterly scan report, which must be completed by a PCI approved ASV.

Larger businesses must do annual on-site assessment completed by a PCI approved QSA and submit the findings to each bank or provider.

It is worth while retaining a copy of any work submitted.

Contact Computer Security Solutions and see how we can help you achieve PCI DSS compliance.

FURTHER INFORMATION

https://www.pcisecuritystandards.org