What is PCI compliance?

If you're wondering exactly what is PCI compliance, the chances are you're one of the many business owners in Australia who've asked themselves this same question. Before answering this question, it's useful to begin by looking at what PCI (and its counterpart DSS) stands for — Payment Card Industry Data Security Standards.

These are a set of requirements that must be followed by all companies and merchants accepting payment from customers via credit or debit card. If you're a business owner or operator and you accept, process, transmit or store cardholder data, then you're required to comply with PCI Security Standards to ensure a secure payment card environment. PCI compliance is expected of all Australian business, irrespective of their size.

The goal of PCI compliance is to ensure that merchants provide the maximum security when processing customer payments or handling customer data. An independent body, named the PCI Security Standard Council (PCI SSC), was created in 2006 to manage and administer the PCI DSS.

This body, however, is not tasked with enforcing compliance and this is primarily the duty of the payment card brands and the acquiring banks, along with retailers and small businesses themselves. Major card brands such as Visa, MasterCard and American Express, played a role in the development of the PCI standards.

In understanding "What is PCI compliance?" one of the key things that business owners are trying to determine is whether or not being compliant is necessary. For the small business owner, the process may seem complicated and time consuming. However, all businesses, big and small, must comply with PCI standards if they plan to accept and process payments via credit or debit cards.

Some of the benefits of following the standards set by PCI compliance include the following:

- Being compliant with the PCI DSS demonstrates that your customers' private information is protected, so they can entrust their credit card payments to you without needing to worry about the security of their data.

- Compliance with PCI DSS enhances your business reputation and is held in high regard by banks and credit card companies — the very same corporations that help you do business and help you to gain customers trust.

- Following the PCI security standards helps you to demonstrate an ongoing commitment to enhance the shopping experience for your customers - and a genuine desire to protect their data by preventing security breaches.

If your business doesn't remain compliant, you may not have the protection you need to prevent your customers' data being accessed without authorisation. A single security breach could do massive damage to your business reputation, which may result in loss of sales and significant loss in profits.

So if you're wondering "What is PCI compliance?" — the answer is this. PCI is a means of building customers' trust and protecting your business against damaging leaks of confidential customer information. Looking after your customers by being PCI compliant will help to ensure continued growth of your business and reinforce goodwill with your customers.

Previously, large organisations processing more than 6 million credit card transactions annually were the only ones required to be compliant. However, it is now mandatory for all merchants, large and small, to become PCI compliant. With this shift making PCI compliance a requirement for all organisations, businesses are advised to begin working toward compliance early on.

Becoming PCI compliant and remaining compliant requires an ongoing commitment to implementing up to the minute procedures and policies for data security. Staff training, technology upgrades and the allocation of resources for both these things will be necessary for many small to medium businesses.

The following tasks are some of the essential things that need to be taken care of to achieve PCI compliance:

1. Building and maintaining a secure network
2. Protecting cardholder data
3. Maintaining a vulnerability management program
4. Implementing strong access control measures

5. Regularly monitoring and testing networks
6. Maintaining an information security policy

In order to operate your business, whether small or large, PCI compliance will be mandatory. If you're unsure how to meet the requirements for PCI compliance, then seeking support from a registered provider of PCI compliance services in Australia is a must. This will ensure that your business has covered all the essentials to pass a PCI compliance audit. It will also mean that you're able to fully protect customer data and card information, helping to reinforce customer confidence and trust.

PCI compliance requirements for Australian businesses

Three core areas businesses should focus on:

Assess, remediate and report

Payment Card Industry (PCI) Data Security Standards (DSS) refer to a set of standards that must be followed by big and small businesses alike when accepting, storing, processing and transmitting customers' credit card information. To be compliant with PCI standards, all business owners, including online retailers, should adhere to 12 PCI compliance requirements for best security practices.

These requirements are in place to protect not only their businesses but also their customers' privacy.

The following are the requirements for PCI compliance:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters. Always change vendor-supplied defaults before installing a system on your network
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks. Use strong cryptography and security protocols
5. Use and regularly update antivirus software. Make sure that your antivirus software remains current and actively running
6. Develop and maintain security systems and applications

7. Restrict access to cardholder data by business employees on a need-to-know basis only
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

Adhering to the above PCI compliance requirements helps businesses to clarify the steps to take in order to maintain a secure payment environment. PCI compliance should be part of an ongoing process of improving security of data, not just a one-time effort. It is useful to continue to strive to remain compliant with the PCI DSS requirements.

There are three core areas of focus for this: Assess, remediate and report.

Assess: Assessing is taking an inventory of your IT assets and the way in which you process your customers' card payment details. The purpose of this is to pinpoint any vulnerabilities that could expose the cardholder to risk. If you're a small business owner and not required to perform on-site assessment to meet PCI DSS compliance, then you may find it useful to complete the Self Assessment Questionnaire (SAQ), to analyse your PCI DSS compliance.

Remediate: Remediation is the process by which vulnerabilities that have been found are corrected or fixed. The process includes scanning your network to spot vulnerabilities, and then classifying and ranking these vulnerabilities so that the most serious are fixed first. This is followed by applying fixes and changes to your processes and workflow, and rescanning to make sure that the vulnerabilities have been fixed.

Report: Reporting is another of the PCI compliance requirements that ensures your business is compliant on a continuing basis. You are required to submit scan reports to your acquiring bank and payment brands that you have business relationships.

Through ongoing commitment to meet PCI compliance requirements, you'll be able to offer security for your customers. If you're operating a large business, it is important that you carry out an on-site assessment once a year; this on-site assessment must be completed by a Qualified Security Assessor (QSA), also assigned by the PCI SSC. By remaining compliant, you can improve your business processes and demonstrate your business professionalism and commitment to client data security.

What changes do we recommend you adopt in your business?

Some simple changes to your business practice should ensure PCI compliance for most professional conference organisers. In addition to implementing points outlined earlier in this document, we suggest you also adopt the below:

- Do not send under any circumstances credit card numbers in body of an email or on an attachment unless you have a method of encrypting outgoing emails. This includes credit card information on hotel contracts.

- Additionally, discourage your clients from sending you copies of anything with credit card detail – you do not want to receive this information unless again the client is able to encrypt outgoing data.

The PCO Association is working with hotels to encourage them to provide secure platforms if they insist on capturing credit card information at contract stage. Using a solid event management system such as EventsAir or similar will enable you to capture, store and transmit delegate credit card details in a secure environment.