

Information Security As Defined By The PCI DSS

By [Andy Eliason](#)

Personal Information is an extremely valuable commodity in today's digital environment. And as consumers become more guarded about using credit cards or anything else that imparts personal data, information security becomes an issue of paramount importance.

The Payment Card Industry realized that in order to create a sense of safe transactions they would need to institute some kind of standardized measures to ensure information security. The companies that made up the Payment Card Industry each had their own standards, but they came to realize that a single standard was more likely to be achievable for most businesses.

The first two requirements of the PCI DSS deal directly with information security. (In truth, every requirement has something to do with security, but due to the direct relation of the first two, those are the requirements this article will focus on.)

Requirement number one states that you must install and maintain a firewall configuration to protect cardholder data. A firewall is a device that allows you to control the computer traffic into and out of your network and around sensitive areas of the system. Unauthorized access must be prohibited. There are often obscure ways that hackers can discover that will allow them to access sensitive information. These avenues must be blocked and a firewall is one of the necessary components to do so.

Establishing a firewall for information security includes some very specific controls such as: a formalized process for approving and testing external network connections and any changes to the configuration. Problems can occur when a firewall is mis-configured, and this is how you can resolve them.

A merchant is also required to provide a current diagram of their network that shows all connections to cardholder data. This is to make sure that no devices or connections are overlooked, because each connection coming into or going out of the network must be firewalled.

Other documentation that is required around information security is a list of services and ports necessary for normal business operations. Justifications for your decisions are also going to be required, including the use of any protocols besides HTTP, SSL, SSH, and VPN, or the reasons behind allowing risky protocols like FTP.

The firewall must be specifically configured to deny all traffic from untrusted sources. This especially applies to any connections between publicly accessible servers and any system that contains cardholder data. These restrictions need to be strictly maintained because hackers are always on the lookout for the smallest hole or slightest chance to exploit a vulnerability, and that is where trouble starts.

Another crucial component of this requirement is to implement IP masquerading. This allows a merchant to have internal addresses that are only available on internal systems. If a hacker could see those IPs they could attempt to access a network with a spoofed IP address.

The second requirement warns merchants not to use vendor-supplied defaults for system passwords and other security parameters. When a vendor provides a system,

there are usually standard passwords that they use. These passwords are very likely well known throughout the hacker communities, and if they are going to attempt to breach your system, these are the first passwords they will try.

For a business to survive in this fast-paced, digital world, information security cannot be taken too lightly. A business might attempt to postpone their PCI compliance, but this can only lead to trouble. As more and more stories of security breaches reach the public notice, more and more consumers are going to demand a certain level of security.

Your choices then are to reach compliance now and provide safe support for your customers, or wait and try to play catch up when they demand compliance before doing business with you. In truth, the choice should not be a difficult one.