

...PCI COMPLIANCE

Any organization that accepts payment card transactions must be in compliance with the PCI (Payment Card Industry) Data Security Standard. Created in response to the increasing problem of security breaches in which thousands of customers have had credit card information stolen or compromised, the standard is the result of a collaboration between major card companies, including MasterCard and Visa, to create a common set of security requirements.

This standard was updated on 1 October 2008 with changes and clarifications on the types of malware organizations need to protect against and the operating systems that need to be covered.

The standard requires organizations to develop policies and implement measures to ensure the secure management of credit card data and controlled access to the networks over which customers' card information is sent. If you fail to comply, you are liable to face significant fines and possible permanent expulsion from card acceptance programs. So if you accept credit or debit card payment, or collect,



1 Build and maintain a secure network

PCI requirements 1 and 2

Controlling access to the network is key to keeping cardholder data safe. Both network and centrally managed personal firewalls should be configured to stop any inbound and outbound traffic that is not specifically required for business and which might compromise your security. In addition, network access control (NAC) solutions ensure that guest computers belonging to, for example, contractors can only access your network if they have a company-approved firewall installed and working.

As well as controlling network and internet connectivity, you need to look at securing the individual computers, adopting industry-accepted hardening standards to ensure that systems are locked after an appropriate period of inactivity and to enforce safer practice over password use. You should ensure that strong passwords are used and changed on a regular basis, and that previously used passwords will be rejected.

2 Protect cardholder data

PCI requirements 3 and 4

Only authorized people should have access to credit card data and, wherever feasible, the number should be truncated so that only part of the number is visible. As a minimum, information on the hard disk should be encrypted so that cardholder information is unreadable if the computer is lost or stolen. You should introduce policies for the safe transmission of credit card information and only encrypted data should be emailed across an open public network. You should ensure that your email gateway policy will result in emails being blocked if unencrypted cardholder data is detected within them.

The loss of sensitive data can also be prevented by locking down ports so that, for example, wireless connectivity is disabled, and by disallowing the use of USB or other mass memory devices.

3 Maintain a vulnerability management program

PCI requirements 5 and 6

You must install endpoint security software on all company-owned Windows and non-Windows computers and ensure it is kept up to date. By creating a robust, centrally managed policy for effective scheduled and on-access scanning, and for the management of security patches on all development, testing and production systems you can ensure you have full visibility and control of the network. Your policy should ensure that the Microsoft patch update service is enabled on all Windows machines. As with the use of personal firewalls, a NAC solution will ensure that guest computers can access your network only if they have company-approved anti-virus software installed, up to date, and running. Ideally, the solution should include a data feed identifying all critical and important patches and perform contextual assessment so that only patches relevant to a given computer are assessed. The web gateway must also be included in any vulnerability management program in order to stop web-borne malware being downloaded onto endpoint computers.

4 Implement strong access control measures

PCI requirements 7, 8 and 9

The use of peer-to-peer remote access software, should be blocked unless there is a clear business need as it creates unnecessary risk. If it is used, each computer must use a unique username and password, and encryption and other security features must be switched on. Choose a security vendor who is able to identify these potentially unwanted applications, and can block their use by unauthorized users.

You should use a NAC solution to prevent unauthorized users accessing any computers, including servers, on which cardholder data might be stored. Use an enforcement mechanism that either blocks access at the network switch using 802.1x or stops the user from getting a valid IP address using DHCP enforcement. Wireless access for guests or business partners should be restricted and any computer not complying with your network access control policy should be quarantined. Any equipment and media containing cardholder data must be physically protected against unauthorized access.

5 Regularly monitor and test networks

PCI requirements 10 and 11

Having installed anti-malware software and intrusion prevention systems to protect against zero-day threats across the network and on endpoint computers, it is essential that you monitor and test that these measures are working. As well as carrying out a continuous vulnerability assessment of all systems on the network, you should also track *all* attempts at access – successful and unsuccessful – and keep records for at least three months. Choosing an endpoint security solution vendor that integrates host intrusion prevention, and a network access control solution that ensures it is properly installed, working and up to date with the latest protection, will help you make your testing a routine maintenance check rather than the beginning of a long fixing process.

6 Maintain an information security policy

PCI requirement 12

Effective compliance with the PCI DSS requires you to create and maintain a full range of processes and security measures for employees and guests as part of a comprehensive information security policy. The security measures in this guide are a good starting point.

THE PCI DATA SECURITY STANDARD

- 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
- 3 Protect stored cardholder data
- 4 Encrypt transmission of cardholder data across open, public networks
- 5 Use and regularly update anti-virus software
- 6 Develop and maintain secure systems and applications
- 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
- 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

Sophos NAC Advanced and Sophos Enterprise Security and Control provide the protection, automation and expertise to protect your business around the clock. To find out more about Sophos products and how to evaluate them, please visit www.sophos.com.