

POLICY

PCI Version 1.1

The standard went through its first facelift and now has an oversight group.

Created two years ago by Visa, MasterCard and other credit card providers, the PCI Data Security Standard was revised in September with the introduction of an oversight body.

The PCI Security Standards Council, founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, was formed to manage the standard going forward. Merchants, payment device and services vendors, processors, and financial institutions can join the council.

The council's first official act was to release version 1.1 of the standard, which clarifies the existing requirements and adds provisions. There had been concern in the security community that the revised standard would be watered down to make it easier for merchants to comply. Instead, the standard was given more teeth.

Perhaps the most noteworthy addition is under Requirement 6—mandating that all custom application code be reviewed for common vulnerabilities by an organization that specializes in application security. Otherwise, a firewall must be installed in front of Internet-facing applications. This will be considered a best practice until June 30, 2008, after which it will be a requirement. Another addition, under Requirement 5, mandates that a company's antivirus software be equipped to uncover spyware and adware, as well as worms and viruses.

The 12 basic requirements remain unchanged. (See box, right.)

BUILD AND MAINTAIN A SECURE NETWORK

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.

PROTECT CARDHOLDER DATA

3. Protect stored cardholder data.
4. Encrypt the transmission of cardholder data across open, public networks.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.

IMPLEMENT 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 TEST NETWORKS

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

MAINTAIN AN INFORMATION SECURITY POLICY

12. Maintain a policy that addresses information security.

—BILL BRENNER