



Compliance Bulletin: Payment Card Industry Data Security Standard Version 1.2

This should not be considered an authoritative list of the changes coming in version 1.2 of the Payment Card Industry Data Security Standard (PCI DSS). The actual changes themselves have not yet been released, only the council's statements about the changes.

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

- Clarified that both firewalls and routers are subject to this requirement and its sub-requirements
- Organizations can now review firewall rules every six months instead of every quarter

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

- References to Wired Equivalent Privacy (WEP) have been removed to emphasize use of Wi-Fi Protected Access (WPA)
- No longer requires disabling of SSID (service set identifier) broadcast, as the effectiveness of this security measure is questionable

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

- As of March 31, 2009 PCI DSS-subject organizations cannot deploy WEP anew and still be compliant
- As of June 30, 2010; all PCI DSS-subject organizations must discontinue the use of WEP and instead use WPA

Requirement 5: Use and regularly update anti-virus software

- Added language to require that all operating systems, Windows or not, must be protected with anti-virus software
- Added language requiring that deployed anti-virus software address all known types of malicious software

Requirement 6: Develop and maintain secure systems and applications

- Changed language regarding the one month timeframe for installing newly released patches, to allow for a risk-based approach
- Requirement 6.6 regarding Web applications will now, without question, be required
 - Any reference to its previous status as a best practice has been removed
 - Custom applications must either undergo a code review or be installed behind an application firewall

Requirement 9: Restrict physical access to cardholder data

- Clarified language to say that off-site storage locations must be visited annually
- Made camera requirement more flexible to allow for other appropriate controls
- Extended definition of media that needs to be secured to include both electronic and paper media that contain cardholder data
- Provided detail on how to properly destroy media that contains cardholder data

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

- Added language requiring that logs from technology that face the outside be copied to an internal server
- Clarified "three months online availability" requirement for audit trail history
- In the event of an incident, audit trail history from the past three months must be immediately available
- It can be available online, from archive or restorable from back up

Requirement 11: Regularly test security systems and processes

- Elaborated on the use of a wireless analyzer to give more guidance
- Changed language to emphasize that both internal and external penetration tests are necessary
- Emphasized that entities must use an Approved Scanning Vendor for quarterly vulnerability scans

Requirement 12: Maintain a policy that addresses information security

- Updated language to require that employees acknowledge that they have read and understood their employer's security policies and procedures at least once a year
- Added language requiring that organizations develop policies and processes by which to manage and monitor their service providers

Because the information about the changes that can be distributed to the public has been limited to the PCI SSC's summary of changes, the table above is far from comprehensive. The changes mentioned are merely those within the PCI SSC's summary that caught the attention of Trustwave. Merchants and service providers should check the final PCI DSS version 1.2 once it is published by the PCI SSC.