

jetNEXUS Payment Card Industry Data Security Standard (PCI DSS) 6.6

What is it?

The PCI DSS 1.1 is a set of requirements designed to enhance payment account data security. The PCI DSS must be met by all organisations that transmit, process or store payment card data.

What does it say?

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and card holder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security

How does this affect Application Delivery Controllers?

ADC's need to be compliant in terms of maintaining a secure architecture as well as providing secure manageability and user access control. In addition, services such as SSL offload need to meet with the PCI DSS requirements.

Requirement 6.6 Code Review and Application Firewalls

There are two options for meeting these criteria.

Option 1 is for Source Code Review:

- Manual review of application source code
- Proper use of automated application source code analyser (scanning) tools
- Manual web application security vulnerability assessment
- Proper use of automated web application security vulnerability assessment (scanning) tools

Option 2 is for Application Firewall (WAFS)

The WAFS device should be able to defend against the OWASP top 10 or PCI requirement 6.5. At the time of writing these are as follows:

(bold is common to both)

PCI DSS Requirement 6.5

- 1) Invalidated input
- 2) Broken access control (for example, malicious use of user IDs)
- 3) **Broken authentication and session management (use of account credentials and session cookies)**
- 4) **Cross-site scripting (XSS) attacks**
- 5) Buffer overflows
- 6) **Injection flaws (for example, structured query language (SQL) injection)**
- 7) **Improper error handling**
- 8) **Insecure storage**
- 9) **Denial of service**
- 10) Insecure configuration management

OWASP Top 10

- 1) **Cross Site Scripting (XSS)**
- 2) **Injection Flaws**
- 3) Malicious File Execution
- 4) Insecure Direct Object Reference
- 5) Cross Site Request Forgery
- 6) **Information Leakage and Improper Error Handling**
- 7) **Broken Authentication and Session Management**
- 8) **Insecure Cryptographic Storage**
- 9) Insecure Communications
- 10) Failure to Restrict URL Access