

Frequently Asked Questions

RETAIL

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Q: What is the Payment Card Industry (PCI) Data Security Standard?

A: The Payment Card Industry (PCI) Data Security Standard is a worldwide standard for consumer data protection across the payment industry. Initially, each card association had its own program to deal with the secure handling of cardholder information – Visa had the Cardholder Information Security Program (CISP) while MasterCard had the MasterCard Site Data Protection Program (SDP). In an effort to create a single approach to safeguard sensitive data for all card brands, Visa and MasterCard aligned their programs to create the PCI Data Security Standard.

Q: What is the benefit of having a single standard?

A: Aligning different security programs under a single standard creates a commonly accepted set of industry tools and measurements as well as a single validation process to satisfy all card associations. This makes the validation process much less complex for the merchant.

Q: What other card companies support this standard?

A: Other card companies operating in the US that have endorsed this standard include American Express, Diners Club, Discover and JCB International.

Q: What are the requirements?

A: The PCI Data Security Standard uses a slightly reorganized version of the original Visa Cardholder Information Security Program (CISP). There are 12 requirements:

- Build and Maintain a Secure Network
 1. Install and maintain a **firewall** configuration to protect data
 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
 3. Protect stored data
 4. **Encrypt** transmission of cardholder data and sensitive information across public networks
- Maintain a Vulnerability Management Program
 5. Use and regularly update **anti-virus software**
 6. Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
 7. Restrict access to data by business need-to-know
 8. Assign a unique ID to each person with computer access
 9. Restrict physical access to cardholder information
- 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



Frequently Asked Questions

Q: Who is required to comply with the PCI Data Security Standard?

A: The PCI Data Security Standard establishes four levels based primarily on the volume of transactions processed annually. The following provides selection criteria, requirements and deadlines by level:

Merchant Level	Selection Criteria	Validation Actions	Validated By	Deadline
1	<ul style="list-style-type: none"> Any merchant - regardless of acceptance channel - processing over 600,000 Visa transactions per year Any merchant that has suffered a hack or an attack that resulted in an account data compromise Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system Any merchant identified by any other payment card brand as Level 1 	Annual On-Site Security Audit Quarterly Network Scan	Independent Security Assessor or Internal Audit if signed by Officer of the Company Qualified Independent Scan Vendor	Sept 30, 2004
2	<ul style="list-style-type: none"> Any e-commerce merchant processing 150,000 to 600,000 Visa transactions per year 	Annual PCO Self-Assessment Questionnaire Quarterly Network Scan	Merchant Qualified Independent Scan Vendor	June 30, 2005
3	<ul style="list-style-type: none"> Any e-commerce merchant processing 20,000 to 150,000 Visa transactions per year 	Annual PCO Self-Assessment Questionnaire Quarterly Network Scan	Merchant Qualified Independent Scan Vendor	June 30, 2005
4	<ul style="list-style-type: none"> All other merchants, regardless of acceptance channel 	Recommended Annual PCI Self-Assessment Questionnaire Recommended Annual Network Scan	Merchant Qualified Independent Scan Vendor	While compliance is mandatory for Level 4, validation is optional but strongly recommended

Q: What are the penalties for non-compliance?

A: Penalties for non-compliance include:

- Possible restrictions on the merchant
- Permanent prohibition of the merchant's participation in Visa programs
- A fine of up to \$500,000 per incident.

For more information please contact retail@sonicwall.com

