

PCI DATA SECURITY STANDARD

The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data. The core requirements are organized in six categories:

PRINCIPLES AND REQUIREMENTS

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 transmission of cardholder data across open, 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 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












VALIDATION ENFORCEMENT

Participating companies can be barred from processing credit card transactions, higher processing fees can be applied; and in the event of a serious security breach, fines of up to \$500,000 can be levied for each instance of non-compliance.

HOW TO VALIDATE COMPLIANCE WITH THE PCI DATA SECURITY STANDARD

To validate compliance, all merchants and service providers, regardless of credit card transaction volume and acceptance channel must fulfill two validation requirements. Some merchants and service providers validate compliance through an Annual On-Site Security Audit and Quarterly Network Scan, while others complete an Annual Self-Assessment Questionnaire and Quarterly Network Scan. Compliance levels for merchants and service providers are defined based on annual transaction volume and corresponding risk exposure:

MERCHANT & SERVICE PROVIDER LEVELS & VALIDATION ACTIONS

	LEVEL	CRITERIA	ON-SITE SECURITY AUDIT	SELF-ASSESSMENT QUESTIONNAIRE	NETWORK SCAN
MERCHANT	1	<ul style="list-style-type: none"> – Any merchant, regardless of acceptance channel, processing more than 6 million transactions per year – Any merchant that suffered a security breach, resulting in an account compromise 	Required Annually *		Required Quarterly 
	2	– Any merchant processing between 1 to 6 million transactions per year		Required Annually 	Required Quarterly 
	3	– Any merchant processing between 20,000 to 1 million transactions per year		Required Annually 	Required Quarterly 
	4	– All other merchants not in Levels 1, 2, or 3, regardless of acceptance channel		Required Annually 	Required Quarterly 
SERVICE PROVIDER	1	– All processors and all payment gateways	Required Annually *		Required Quarterly 
	2	– Any service provider that is not in Level 1 and stores, processes or transmits more than 1 million accounts / transactions annually	Required Annually *		Required Quarterly 
	3	– Any service provider that is not in Level 1 and stores, processes or transmits less than 1 million accounts / transactions annually		Required Annually 	Required Quarterly 

* On-Site Security Audits may be conducted through Qualys PCI Consulting Partners - <http://www.qualys.com/partners/pci>