

# PCI DSS Compliance and the Barracuda Backup Service

In response to the increase in identity theft and security breaches, major credit card companies collaborated to create the Payment Card Industry Data Security Standard (PCI DSS) for merchants, processors, and point-of-sale providers handling and storing sensitive account information. PCI DSS is a standard that is applied to organizations and their security practices rather than to individual products. Though the Barracuda Backup Service is not a component of credit card processing transactions and is not directly storing credit card processing data, Barracuda Networks recognizes that some customers may choose to back up sensitive information.

Organizations processing credit cards and storing credit card information are responsible for establishing, testing, and maintaining security practices that keep sensitive information safe. While there are no penalties levied by the PCI Security Standards Council responsible for managing the requirements, credit card issuers and financial institutions can enforce PCI DSS compliance by offering incentives and issuing fines. The current PCI DSS Version 1.2 outlines 12 procedures and system requirements to secure Primary Account Number (PAN) information.

## Payment Card Industry Data Security Standard (PCI DSS) Requirements

The 12 PCI DSS requirements are organized into six main categories and mandate the proper use of firewalls, message encryption, access controls, network monitoring and the need for an information security policy. To be fully compliant, an organization must satisfy all 12 requirements.<sup>1</sup>

### Maintain a Secure Network: Requirements 1 and 2

- 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: Requirements 3 and 4

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

### Maintain a Vulnerability Management Program: Requirements 5 and 6

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

### Implement Strong Access Controls: Requirements 7, 8, and 9

- 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: Requirements 10 and 11

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

### Maintain an Information Security Policy: Requirement 12

- Maintain a policy that addresses information security

## Barracuda Backup Service Security Measures

While there is no PCI certification process for products, as a Web security company, Barracuda Networks takes these guidelines very seriously. Customers who have gone through their own PCI DSS compliance process understand that PCI does not mandate that they store credit card data, but does mandate that sensitive data is stored in a secure, encrypted manner.<sup>2</sup> Any data stored on the BBS will also be behind the corporate firewall and will be protected by network security measures validated by PCI DSS. With the Barracuda Backup Service, you have the option to maintain as much of that sensitive data onsite as you like. In addition, the Barracuda Backup Service offers the following security features to protect all data that is backed up and sent offsite.

RELEASE 1  
DECEMBER 2009

- Before being sent offsite, data is encrypted using a very secure combination of both AES 256 bit and RSA 1024 bit algorithms.
- Data is transferred to and from Barracuda Networks data centers using two layers of 256 bit encryption.
- Access to data is determined by your Barracuda Backup Server administrator.
- Storage devices at the Barracuda Networks data centers are on a secure network protected behind firewalls.
- All transfers of backup data into and out of Barracuda Networks cloud storage are encrypted and authorized.

For more information about PCI DSS Compliance, please visit the PCI Security Standards Council Web site at <http://www.pcisecuritystandards.org>.

<sup>1</sup> "About the PCI Data Security Standard (PCI DSS)" PCI Security Standards Council [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

<sup>2</sup> "Ten Common Myths of PCI DSS" PCI Security Standards Council LLC [https://www.pcisecuritystandards.org/pdfs/pciscc\\_ten\\_common\\_myths.pdf](https://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf) June 2008

*For questions about the Barracuda Backup Service, please visit <http://www.barracuda.com/backup> or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit <http://www.barracuda.com/products>.*

### **About Barracuda Networks Inc.**

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif. For more information, please visit [www.barracudanetworks.com](http://www.barracudanetworks.com).



**Barracuda Networks**

3175 S. Winchester Boulevard

Campbell, CA 95008

United States

+1 408.342.5400

[www.barracuda.com](http://www.barracuda.com)

[info@barracuda.com](mailto:info@barracuda.com)