



Payment Card Industry (PCI) Data Security Standard

Requirements and Security Assessment Basics – Version 1.2

The payment card industry compliance and validation regulations apply to financial institutions, Internet vendors and retail merchants. The rules spell out what security measures must be taken to protect the private information of employers and employees during any transaction occurring with the use of a paycard. They also require certain auditing procedures. The Payment Card Industry (PCI) Data Security Standard (DSS) is used by all card brands to assure the security of the data gathered while an employee is making a transaction at a bank or through a participating vendor.

In the wake of high-profile identity theft and fraud concerns, VISA and MasterCard are now requiring organizations that process cardholder data to comply with their PCI Data Security Standard. PCI details twelve key requirements designed to reduce the risk from the electronic transmission of cardholder data, and devotes substantial focus on the development and maintenance of secure systems and applications.

Payment Card Industry (PCI) Data Security Standard (DSS) v1.2

Category	Requirement
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 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 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

There are four merchant categories:

- Level 1. Merchants with more than 6,000,000 transactions per year. Other merchants in Level 1 will be merchants whose security has been violated and data compromised and merchants which another credit card company has classified as Level 1.
- Level 2. Merchants with 150,000 to 6,000,000 transactions per year.
- Level 3. Merchants with 20,000 to 150,000 transactions per year.
- Level 4. Merchants with less than 20,000 transactions per year.

PCI Compliance Validation

Credit card companies validate that vendors are abiding by the PCI Compliance regulations. The volume of transactions and the risk determined by the credit card company determines the validation rating for the merchants and institutions accepting credit/debit and paycards. Along with requiring participating businesses to complete a self-assessment questionnaire, MasterCard and Visa perform the following actions to validate a participating business' security:

1. An on-site visit
2. A network scan performed by an authorized PCI Compliance scanning vendor

How Blue Ridge Networks VPN assists with PCI Compliance

Blue Ridge Networks Secure Virtual Ethernet Services (SVES) managed service assists with complying with PCI Requirements #1 (if using optional Collocation Firewall) and #4.

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

Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' email access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS Requirements

- 1.1 Establish firewall and router configuration standards.
- 1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.
Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage
- 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

Blue Ridge Networks Compliance Response

Blue Ridge deploys a VPN Device called a Remotelink at the stores/remote sites. This device sits at the border of the store's network and encrypts all traffic in and out of the store. The traffic is transmitted through a secure tunnel to a VPN concentrator called a BorderGuard, located at a secure collocation facility. This secure device does not allow any unencrypted traffic in or out of the store.

If an employee wishes to browse the Internet, the traffic is encrypted and sent through the secure tunnel to the collocation facility. There, the packets are decrypted, and sent to the firewall if destined to the Internet, or encrypted and sent to HQ if applicable. There is no direct Internet access through the store.

The firewall maintains a white list of acceptable sites and their URL addresses. Only traffic destined to one of these sites is allowed through the URL filter on the firewall; all other sites are blocked.

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

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements

4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in the scope of the PCI DSS are:

- *The Internet,*
- *Wireless technologies*
 - *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.*
 - *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*
- *Global System for Mobile communications (GSM), and*
- *General Packet Radio Service (GPRS).*

4.2 Never send unencrypted Primary Account Numbers (PANs) by end-user messaging technologies (for example, email, instant messaging, and chat).

Blue Ridge Networks Compliance Response

Blue Ridge devices, both the RemoteLink and the BorderGuard, use strong cryptography. The specifications are as follows:

- Cryptography: Data Privacy Facility (DPF)
- Encryption algorithm: AES 256
- Data integrity: HMAC SHA-1
- Public Key cryptography: RSA and Diffie-Hellman, 1024 bit keys

Each packet received by either of the VPN devices is authenticated; the VPN system uses bi-directional IPSEC tunnels.

No data is sent from the store without entering the VPN tunnel, including email, instant messaging, and chat applications.