worldpay

worldpay.com

Understanding the 12 requirements of PCI DSS

SaferPayments

Be smart. Be compliant. Be protected.

The 12 requirements of the Payment Card Industry Data Security Standard (PCI DSS) by type

Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

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

If you choose to process, store or transmit cardholder data via the internet you'll need to demonstrate that your firewalls and routers are securely configured and independently tested.

A firewall is a fundamental part of network security. A correctly configured firewall will comply with this requirement and you'll need to verify this through the Security Assessment Questionairre.

An important part of securing your network, is to make sure all accounts and setting are changed from default and configured to a secure standard.

Protect cardholder data

3. Protect stored cardholder data

4. Encrypt transmission of cardholder data across open, public networks

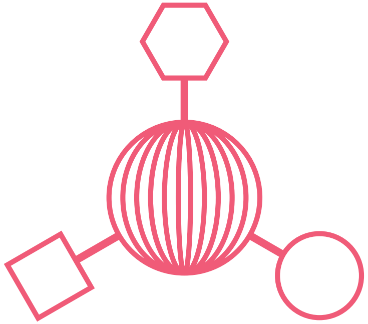
It's important to protect any cardholder data in a physical or online format.

All stored data must be encrypted and sensitive data is never disclosed or stored after authorisation (e.g. PIN numbers and the full card details on the magnetic strip).

You'll also need to make sure your business is not using public networks to transfer data.

If you are storing, transmitting or processing cardholder data across open public networks (Including the internet), you need to ensure you are using the strongest form of encrypting to protect it.

Maintain a vulnerability management program



5. Use and regularly update your antivirus software

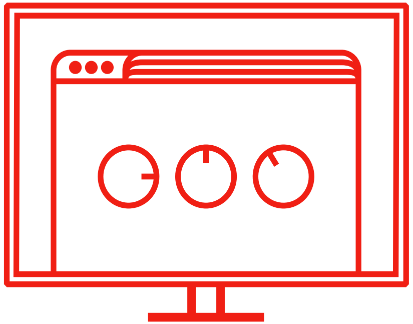
6. Develop and maintain secure systems and applications

Keep your customer's data and your business' computer system safe by installing antivirus software. Scans will need to run regularly and software kept up to date.

You'll need to regularly update this to ensure you're protected from all online threats. And if you develop or write any applications or programs you will need to remain vigilant against ongoing threat and vulnerabilities, through testing and maintenance.

worldpay

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

Make sure you're controlling who can access your customers' card details. You should only allow access to employees who need to know this information.

You can do this by assigning unique IDs with different access permissions to each employee on your computer system.

Make sure to keep any physical records locked away with the keys provided to those who need it. Physical media needs to monitored and destroyed when no longer needed.

Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Regularly check your network for vulnerabilities by running internal and external vulnerability scans.

You'll also need to track and monitor who is accessing your network and cardholder information so you can identify and act on any unusual activity.

Maintain an information security policy

12. Maintain a policy that addresses information security

To make sure your business keeps all cardholder details safe, create and maintain an information security policy.

You are required to set a security policy that lets all employees know what is expected of them and what they must follow.