PCI COMPLIANCE

Can I use Darkspire Hosting to host an eCommerce site?

Yes! But only with appropriate eCommerce software.

No matter where you host your website, including your eCommerce site with products and shopping carts, you must never allow credit card data to pass through your website. That includes credit card numbers, expiration dates, CCV numbers, and so on. The reason is that doing so requires you to maintain compliance with a complex and expensive system called PCI-DSS, described in more detail below.

Fortunately it's easy to have an eCommerce site that doesn't actually process credit card data, and therefore doesn't need to be PCI-DSS compliant. All you need to do is use an external credit card processing system, which many of the existing WordPress eCommerce systems already support. There are many such 3rd-party processors, and Darkspire Hosting holds no opinion on which you choose. That is, we neither recommend nor block those processors. Examples of these sorts of processors include but certainly aren't limited to: Authorize.NET, PayPal, Stripe, Braintree, Recurly, and Chargify.

Similarly, we neither recommend nor block many eCommerce solutions for WordPress, which integrate completely with your website for product directories, shopping carts, and so forth, and then use one or more of those 3rd-party processors for the credit card processing. Examples of those systems include but aren't limited to: WooCommerce, Cart66, Shopp, WP eCommerce, GetShopped, and MarketPress.

Is Darkspire Hosting a PCI-DSS compliant solution?

As long as no payment card data is stored, hosted, or otherwise processed by Darkspire Hosting, then Darkspire Hosting is compliant with PCI-DSS requirements. It is your responsibility to ensure

that no such data is brought onto the Darkspire Hosting system. Please refer to the information in this FAQ for more information, or contact our tech support with any questions.

Furthermore, although we get this question a lot, in fact it's not possible for a web-host to itself be "PCI compliant." The reason is that compliance requires many things, including how you, the customer, control access to your site, what precautions you have on your source code, how you store data on disk and in your database, run certain kinds of security scans, transmit data across public networks, and so on. The bulk of these requirements are the responsibility of the site owner, as opposed to the physical web host. Therefore the host itself isn't close to sufficient to be "compliant."

Darkspire Hosting does have internal policies and procedures around human access, logging, security practices, physical access practices, and so on, which are a part of being PCI compliant but which don't "make you compliant" automatically as a customer.

Because "compliance" is something that you as the customer are ultimately responsible for, and because any web host is limited in how it contributes to that compliance, we always recommend that you architect your site to not require PCI compliance at all, relying instead on services such as the ones listed above for all sensitive payment data, and thus alleviating the need for you to achieve compliance, and being more secure in the process.

What IS PCI?

Payment Cards Industry (PCI) is collective of businesses associated with Credit Card providers, Debit Card providers, Credit Card/Debit processors, and card pre-pay providers.

Do clients need to be PCI Compliant?

According to PCI DSS Compliance, any client that accepts credit card information or does a credit card transaction on their site will need to be PCI Compliant or put themselves under "high risk" and liability from the different credit card providers.

A client can remain in compliance if they perform CC transactions via a third party service, where the transaction is submitted and processed entirely through a separate service. A good example would be Authorize.net DPM, Braintree's API service, and PayPal Pro's API. These type of services process CC transactions through a client-side browser request – thus allowing these payment processors to handle the payments entirely through their system. These processors maintain their own PCI compliance so a client does not need to do their own auditing.

What is the PCI Security Standards Council?

The PCI Security Standards Council (PCI SSC) is a global forum, founded in 2006, uniting the major credit card providers (MasterCard, American Express, Visa, etc.) to set standards of accepting and processing credit card data. According to the PCI SSC Standards overview, there's a set of requirements called the Payment Card Industry Data Security Standard (or "PCI DSS") and it was developed by the PCISSC – (the Payment Card Industry Security Standards Council)

These requirements are designed to provide a standardized set of consistent security measures for merchants to follow that are handling credit card transactions.

The standard includes 12 requirements for maintaining a secure operation:

Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes
- Maintain an Information Security Policy
- Requirement 12: Maintain a policy that addresses information security

For WordPress your E-commerce options are limited, and for a PCI Compliant shopping cart, they're limited even further.