PCI DSS Compliance

What is PCI DSS?

Developed by the major credit card issuers, the Payment Card Industry Data Security Standard (PCI DSS) outlines best practices for credit card data storage, processing and transmission. Its intent is to protect credit card information from fraud, theft, or any other breach.

What is the impact of PCI DSS?

Any retailer, merchant, bank, or service provider storing, processing or transmitting cardholder data must comply with PCI DSS. Compliance validation is required for major merchants and may be required for some smaller merchants. Failure to comply with PCI DSS could result in fines that are severe enough to put you out of business.

What are the requirements of PCI DSS?

Here are twelve specific requirements that can be grouped into six main categories which retailers must meet to comply with PCI DSS:

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 or programs
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 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 for all personnel

How do companies comply with PCI DSS?

In order to comply with PCI DSS, companies must meet all 12 requirements mentioned above. Essentially, protecting cardholder information and protecting IT infrastructure are the two main points of PCI DSS. To protect cardholder information companies must protect the data wherever it travels, specifically encrypting it over public networks. In addition to encryption, companies must put into place IT security controls to protect the cardholder's data from hackers and other cyber criminals who want to steal the information. To protect IT infrastructure, merchants must protect both systems and applications. In addition, they must establish control processes and guidelines to secure computers and other electronic equipment.

How does Certes Networks help you comply with PCI DSS?

Our approach of "deny everyone, permit by exception" protects both your network and your data. CryptoFlow® Creator enables secure data transmissions, which assures the confidentiality, authenticity and integrity of data as it travels across any network, regardless of size, type or topology. Our solutions provide you with encryption and authentication of all data, including cardholder information. CryptoFlow Creator also provides authentication of endpoints and data packets. Acting as a cryptographic firewall that rejects any packets lacking the proper authentication, CryptoFlow Creator ensures access to data is limited to those who need to see it. By protecting the network and the data, we help you comply with PCI DSS.

PCI Requirement	Resolution	How Certes Networks Helps
Scope of PCI assessment may include the entire network.	Limit the scope of the Cardholder Data Environment (CDE) by segmenting the network. Isolate systems that store, process or transmit cardholder data.	■ We help you reduce scope while avoiding major network changes by overlaying encryption on top of the existing network ■ We provide strong cryptography to isolate the CDE from the rest of the network ■ Our solutions rapidly reduce scope by encrypting among network segments that store, process or transmit cardholder data ■ You save money during initial PCI assessment and with ongoing reassessments by reducing the scope of the assessment. ■ We make encryption easy to deploy and manage with simple GUI-based policies and encryption that allows the network headers to pass in the clear while encrypting the payload Certes Networks uses strong cryptography and simple and flexible policies to isolate areas of the network without changing the physical or logical network topology. CryptoFlow solutions can be deployed quickly to provide a secure overlay that isolates the Cardholder Data Environment from the rest of the network. This protection is stronger than traditional firewall-based approaches because it isolates the network using encryption rather than relying only on the packet headers. ■ Furthermore, it eliminates the need to re-architect the network or replace legacy applications - CDE networks can be interconnected over your existing network infrastructure with complete cryptographic isolation that takes the rest of the network out of scope.
Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks	Encrypt cardholder data over any network that is outside of your control. This includes: Internet, GSM, GPRS, MPLS, VPLS or carrier Ethernet networks operated by a third party service provider.	■ We encrypt data as it traverses a third party service provider network or the Internet ■ Our solution is a "drop-in" solution that works with existing network and applications ■ Works with your existing networks without getting in the way of existing failover, redundancy and load-sharing ■ Certes Networks can quickly and simply encrypt card-holder data and other sensitive information across any network without affecting the applications and services that run over the network.
Track and monitor all access to network resources and cardholder data	Provide logging and auditing to track user activities.	■ Full audit trail for logging and auditing ■ Role-based access allows for an "auditor" role to monitor security ■ Auditing and monitoring can be easily outsourced to a third party

Certes Networks Zero Trust Security solutions protect data and applications in motion with a range of software defined security solutions. Our Zero Trust framework protects application traffic over any environment to any user, device or location; all this without affecting network or application performance whatsoever. Our patented and industry leading layer 4 stealth encryption solution gives you "Encryption Without Compromise".

**Find out how Certes CryptoFlow Solutions will revolutionize how you secure data in motion.
Visit CertesNetworks.com**