atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

PCI HOSTING REQUIREMENTS

The PCI Security Standards Council comprises the major credit card companies, including Mastercard, American Express, Visa, and Discover. The PCI Security Standards Council sets the standards for how organizations should securely handle credit card payments and data, known as the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS applies to any company processing, transmitting, or storing credit card information. PCI-DSS was created to reduce fraud and the chance of cyberattacks. Achieving PCI DSS compliance is not an easy task, but the benefits of achieving it are highly rewarding. A secure Card Data Environment (CDE) must be created to gain compliance.

Did You Know?

Fines of $5,000 to $100,000 per month for compliance violations are possible under PCI DSS.

THE 12 REQUIREMENTS OF PCI-DSS

While PCI DSS outlines 12 operational and technical requirements to protect cardholder data, **there are over 250 sub-requirements and over 400 testing criteria to achieve PCI-DSS compliance.**

Install a firewall	You must install, harden and maintain network firewalls to secure the environment. The firewall must be configured to filter incoming and outgoing traffic, and access rules must be reviewed at least twice a year.
Avoid default passwords	Harden your systems and devices by maintaining secure passwords and usernames. Change default system credentials as these are easy to guess and readily available on the Internet.
Protect stored payment card data	The most crucial rule of the PCI DSS is to secure all cardholder data. You must know what data is stored and for how long. It must use encryption and robust key management. Data can also be hashed, truncated, or tokenized.
Encrypt cardholder data transmission	Cardholder data must be encrypted before it is transmitted (TLS, IPSec, and SSH) and decrypted once it has arrived. Strong security and cryptography protocols are a requirement for preventing data theft.
Deploy up-to-date antivirus software	A vulnerability management program must be used to identify payment card system vulnerabilities. This involves installing an antivirus solution across all systems and devices and keeping it updated. The antivirus must remain active at all times, use up-to-date dictionaries, and generate auditable logs.
Maintain secure applications and systems	To reduce the potential for exploits, organizations must build and maintain secure applications. Security patches should be applied immediately upon release, where possible. Organizations must also be able to discover and rank new vulnerabilities, with all new or modified code checked for known and unknown vulnerabilities.
Restrict access to cardholder data	Cardholder data should only be accessible on a need-to-know basis and must be managed with an access control system that allows or denies access according to specified roles and permissions.
Implement user access identification	All users should be assigned unique, complex usernames and passwords, which must never be shared. Access identification should be based on individual users, not groups. This not only provides an extra layer of security but also ensures traceability in the case of a data breach. It is recommended to implement multi-factor authentication (MFA).
Protect data physically	Access to physical objects (i.e servers, workstations, and paperwork) must be restricted. Organizations are required to protect physical data storage locations with electronic monitoring and video cameras, signed access logs, and 24x7 recording.

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS

atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

PCI HOSTING REQUIREMENTS

Monitor network access	Network systems must be monitored constantly, with network activity logs recording access. Tools like Security Information and Event Monitoring (SIEM) can assist with system activity logging and monitoring. It is important to keep time-synchronized records for at least a year to provide an audit trail.
Tests systems and processes on an ongoing basis	Continuous testing is essential for protecting systems and processes against malicious exploits of newly discovered vulnerabilities. This includes vulnerability and penetration testing, as well as periodic scanning by a wireless analyzer to identify vulnerable access points.
Implement an information security policy	You must create, implement and maintain a company-wide infosec policy, covering management, staff, and 3rd parties. This policy must be reviewed annually and communicated to all relevant parties.

PCI-COMPLIANT HOSTING AND THE SHARED RESPONSIBILITY MODEL

If your organization takes credit card payments, you need to make sure that your software and infrastructure adhere to PCI DSS standards. If your company employs a 3rd party payment processor, you are still accountable for ensuring PCI DSS compliance.

PCI-compliant hosting providers have the infrastructure and expertise to help organizations obtain PCI compliance easily and cost-effectively.

You should understand PCI DSS compliance as a joint responsibility. A PCI-compliant hosting provider can assist your organization in achieving compliance, but both parties need to work together to realize this goal.

PCI DSS Compliance Doesn't End with PCI-Compliant Hosting

Even if you select a PCI-compliant hosting provider, you still retain responsibility for your organization's compliance with PCI. Take into account the following considerations:

- **Know your vulnerabilities** - evaluate applications and assets for secure configurations, isolate outdated software, use security patches, and deal with security flaws in custom applications.
- **Keep up-to-date, well-documented procedures** - business objectives, requirements, incident response plans, assets, and other items vital to PCI compliance might vary in an instant. Without proper management and governance procedures, organizations won't recognize when they are not in compliance.
- **Ensure third-party service providers are compliant** - it is your responsibility to ensure that third-party service providers provide the required level of compliance and ensure that they maintain compliance over time.
- **Providing timely information** - generating reports for PCI compliance in a timely way is also challenging. This is particularly true when various data types need to be combined and communicated in a significant manner to various audiences.

Simple Signup Process

You can start your PCI Compliance journey right now by emailing **sales@atlantic.net**. If you have any questions, please get in touch! Contact an advisor at **+1-408-335-0825**

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS