Compliance Brief

Payment Card Industry Data Security Standard (PCI DSS) v4.0.1

What is PCI and why is it Important?

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. 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.

Specific Requirements for Compliance

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

Additional Requirements for v4.0 release

Timeline for adoption:
2024: The deadline for organizations to fully transition to PCI DSS v4.0.
2025: Several new requirements will become mandatory, including the expanded use of multi-factor authentication and encryption updates.

New and enhanced requirements introduced in PCI DSS v4.0

Increased focus on risk management: Organizations must define and perform risk assessments to understand and address emerging threats.

• **Enhanced authentication methods**: Increased adoption of multi-factor authentication (MFA) for all non-console administrative access and remote access to the cardholder data environment (CDE).

• **Expanded encryption requirements**: Emphasis on stronger cryptography standards and protection of sensitive authentication data.

• **Customization for security requirements**: Organizations can implement customized security controls if they achieve the same level of protection as the defined standards.

How Certes DPRM Helps you achieve PCI compliance

"Certes DPRM effectively **reduces the scope of PCI DSS compliance** by segmenting data flows through strong cryptography. It ensures that **cardholder data (CHD) is protected during transmission**, simplifying compliance efforts."

Simon Turner – (CISSP, CISM, CISA, VCP, ISA) Senior Member of ISSCA Consultancy Services, BT Group and PCI QSA (Qualified Security Assessor)

Penalties

Monthly fines of $5,000 to $100,000 for non-compliance.

- Potential penalties of $50 to $90 per compromised card in the event of a data breach.
- Increased transaction fees and potential loss of processing privileges.
- Reputational damage and customer loss.
- Legal and regulatory implications, especially in regions with data privacy laws.

To avoid these penalties, organizations should ensure they remain compliant with the latest PCI DSS standards, implement robust security measures, and undergo regular audits or assessments to identify and address any gaps in compliance.

What to do for Compliance

In order to comply with PCI DSS, companies must meet all 12 requirements mentioned above. Essentially, protecting cardholder information and processing 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 cybercriminals 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.

certes.ai
+1-412 262 2571
info@certes.ai