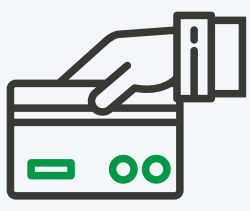
TOP 8 PCI DSS COMPLIANCE TIPS

PCI DSS standards were created to protect credit cardholders' data from **theft** and **fraud**. Any organization that accepts **credit card payments** must comply with these standards. Failing to meet these standards can result in **fines, loss of reputation,** and **even legal action**.

Here are eight tips for meeting and staying PCI DSS compliant.

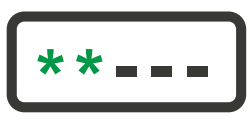


1. Understand the Scope of PCI DSS Requirements

Knowing what systems, applications, and devices in your organization are in scope and need to comply with the standards is crucial.

2. Keep Your Systems Updated and Patched

Make sure to install all the necessary security patches for your operating systems, software, and applications to avoid vulnerabilities.



3. Use Strong Passwords and Multi-Factor Authentication

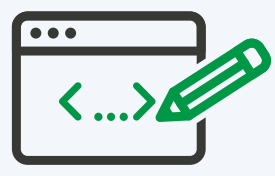
Use strong passwords and multi-factor authentication to protect access to your systems and data.

4. Use Encryption to Protect Sensitive Data

Use encryption to protect sensitive data such as credit card numbers, social security numbers, and other personal information.

5. Limit Access to Sensitive Data

Limit access to sensitive data to only those who need it to perform their jobs.



6. Monitor and Log All System Activity

Monitoring and logging all system activity can help quickly detect and respond to security incidents.

7. Perform Regular Vulnerability Scans and Penetration Testing

Performing regular vulnerability scans and penetration testing can help identify potential vulnerabilities in your systems and applications.

8. Develop And Maintain a Security Policy

Develop and maintain a security policy that outlines your organization's security measures and procedures.

Secure Coding Training to Meet Your PCI Compliance Goals

Outside of general risk remediation, there are specific requirements that secure coding training can help you meet within the PCI DSS framework.

PCI DSS Requirement 6.5.1 mandates that all custom code developed for payment systems must be reviewed for security vulnerabilities.

Secure coding training can help developers learn how to write more secure code by avoiding common coding errors that can lead to vulnerabilities in the system.

PCI DSS Requirement 6.5.2 mandates that organizations implement a process to ensure that any security vulnerabilities found during the code review process are addressed in a timely manner.

Secure coding training can help organizations develop this process by training developers on how to identify and remediate security vulnerabilities in code.

PCI DSS Requirement 12.6 mandates that organizations implement a security awareness program that includes training for all personnel.

Rather than creating a program from scratch, your organization can partner with a team of experts with all the resources you'll need.

Read the Full Article on our **Website** and **Try Our Training**

We help enterprises reduce vulnerabilities with application security education for developers and all individuals involved in creating software. Development teams are empowered through practical, skill-oriented secure coding training that easily satisfies compliance needs and goes beyond to build a security-first development culture.

www.SecurityJourney.com | +1 (804) 742-2533 | info@securityjourney.com