



Understanding PCI DSS Compliance: A Comprehensive Guide

Presented by:

VirtualPostMail (VPM)

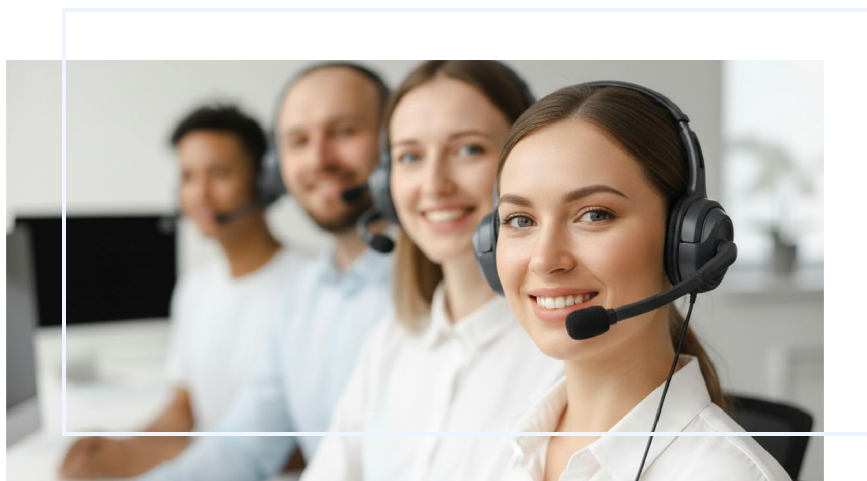
Website

www.virtualpostmail.com

Introduction



Protecting customer data is critical. A single breach can result in devastating financial and reputational consequences. PCI DSS ensures consistent security for anyone who processes cardholder data.



What is PCI DSS?

PCI DSS is a global framework of security requirements designed to ensure that organizations handling credit and debit card data do so in a secure manner.

The Cost of Non-Compliance

- Loss of ability to process payments
- Hefty regulatory fines and penalties
- Mandatory forensic investigations
- Liability for fraud and legal exposure
- Long-term reputational harm

Compliance Checklist

1. Assess: Identify systems touching data
2. Repair: Address gaps and vulnerabilities
3. Report: Formally document your compliance



PCI DSS Requirements



PCI DSS is built on 12 core requirements, organized into six security objectives. Together, they provide a comprehensive approach to protecting payment data across your entire organization.

How Digital Mailrooms Help

- Secure physical access to facilities
- Encryption of data in transit and rest
- Audit logging and access monitoring
- Two-factor authentication (2FA)
- Retention and secure disposal policies





Security Goals

Build and maintain a secure network and systems to protect cardholder data through strong firewalls and customized settings.



Data Protection

Implement strong access control measures and regularly monitor and test networks to detect unauthorized access.

Conclusion

PCI DSS provides an effective framework for protecting data. Integrating secure mail handling into your program eliminates blind spots and builds customer trust. With VPM, you can be sure your documents are protected.



909-235-6245



help@virtualpostmail.com



www.virtualpostmail.com