










Secure File Sharing Best Practices for PCI Compliance



To securely share card holder data in adherence to PCI DSS requirements, businesses need to implement critical security measures to avoid costly violations. By following these practices, organizations can securely share credit card data with trusted partners while maintaining PCI DSS compliance.

-  **1. Use data encryption:** Encrypt all sensitive cardholder data before transmission using strong cryptography and security protocols like transport layer security (TLS) 1.2 or higher.
-  **2. Implement secure file transfer:** Utilize advanced security protocols such as SFTP or FTPS to transmit encrypted card data files between partners.
-  **3. Limit data elements shared:** Only share the minimum cardholder data elements necessary. Avoid sharing sensitive authentication data like CVV codes.
-  **4. Employ data tokenization:** Replace credit card numbers with unique tokens before sharing data with partners to reduce risk.
-  **5. Establish formal agreements:** Create written agreements with partners detailing security responsibilities, access controls, and data handling procedures.
-  **6. Restrict access:** Limit access to cardholder data to only those individuals who need it to perform their job functions.
-  **7. Monitor data access:** Implement monitoring and audit logs to track all access to shared cardholder data by partners.
-  **8. Conduct partner assessments:** Regularly assess partners' PCI DSS compliance and security controls to ensure they meet requirements.
-  **9. Securely delete data:** Implement processes to securely delete or destroy cardholder data when no longer needed by partners.

