cisco Webex

Security always matters.

PCI DSS and why security always matters

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards created to safeguard all companies that accept, obtain, process, save, or transmit credit card information—because security always matters. It's important to know the latest regulations and mandates and how they may impact you. The following list of important issues will help keep you safe out there.

PCI DSS applies to any organization that processes online transactions via the Internet.

PCI DSS applies to organizations of all sizes with any number of online transactions that accept, pass on, or store cardholder information. This could be via the phone, Internet, or any other means.

Your company may need vulnerability scanning to validate compliance.

If you qualify for certain self-assessment questionnaires (SAQs) or if you electronically store cardholder data post authorization, a quarterly scan by a PCI Security Standards Council (SSC) Approved Scanning Vendor (ASV) is required to maintain compliance.

Merchants that suffer a data breach may be escalated to a higher validation level.

All merchants will fall into one of the four validation levels based on Visa transaction volume over a 12-month period. Any merchant that has suffered a breach that resulted in an account data compromise may be escalated to a higher validation level.

Small-to-medium-sized businesses must regularly validate compliance.

All businesses need to validate compliance and complete and obtain evidence of a passing vulnerability scan with a PCI SSC ASV.

Prepaid cards are protected under PCI.

In-scope cards include any debit, credit, and prepaid cards branded with one of the five card association or brand logos that participate in the PCI SSC. American Express, Discover, JCB, Mastercard, and Visa International are protected under PCI.

Source: https://www.pcicomplianceguide.org/faq/

Types of voice over IP (VOIP) traffic potentially affected by PCI DSS:

- VoIP traffic that contains payment card account data
- Call recording management and storage that includes payment card account data
- Control of the agent or caller interface within the physical call center space when payment card account data is exchanged

What's next

The PCI SSC recommends upgrading to Transport Layer Security 1.2 (TLS 1.2) or higher as soon as possible to demonstrate strong cryptography.

If an organization is found to be noncompliant, it could be fined from US$5000 to US$100,000 per month.

Learn more to find out if this regulation could be impacting your business.

cisco.com/go/voipcompliance