PCI compliance is the process of following the Payment Card Industry Data Security Standard (PCI DSS), a collection of security guidelines created to guarantee that every business that handles credit card data keeps a safe environment. PCI DSS establishes guidelines for the processing, transmission, and storage of cardholder data in an effort to prevent fraud and theft.

This is applicable to merchants, service providers, and third-party vendors, as well as any other business that handles, saves, or transmits credit card information. To safeguard cardholder data, security criteria are established by the PCI Data Security Standard (DSS). The amount of transactions determines the compliance requirements, with larger businesses subject to tougher restrictions.

It is important to note that PCI compliance aids companies in safeguarding private client information and avoiding fines, harm to their reputation, and legal repercussions associated with data breaches.

We are writing this article to ensure that everyone is aware that in June 2024, the Payment Card Industry Data Security Standard (PCI DSS) was updated to version 4.0.1. To improve effectiveness and usability, this version has a few small clarifications and fixes. Released in March 2022, PCI DSS v4.0 gave enterprises until March 31, 2024, to upgrade from version 3.2.1 to 4.0.

In order to guarantee that all businesses processing credit card information maintain a secure environment, PCI compliance refers to following the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS establishes standards for data processing, transmission, and storage in an effort to prevent fraud and theft of cardholder information.

Twelve primary PCI compliance criteria are broken down into six overarching objectives, including:

- To protect cardholder data, a secure network should be built and maintained by putting firewalls, routers, and other security measures in place
- Protect Cardholder Data by encrypting stored cardholder data and transmitting data using robust encryption techniques
- Keep up a vulnerability management program by routinely upgrading systems and software to avoid security flaws
- Making sure that only those with permission can access cardholder data is known as access control
- Frequent Testing and Monitoring: Testing security systems and keeping an eye out for questionable activities on networks
- Maintain an Information Security Policy: Creating and upholding data security guidelines for the entire company

Please note that as of April 1, 2025 our 4.10 compliance will be updated to 4.2 compliance. In the past PCI compliance used to only apply to those who held the data. However, now this change affects everyone who takes credit card payments as it applies to everyone who has a stripe for credit card payments.

As v3.2.1 was retired as of March 31, 2024 PCIDSS it is essential that everyone updates their compliance.

PCI DSS version 3.2.1 should no longer be used since it has been formally deprecated. Using out-of-date standards could result in security concerns and non-compliance with the most recent best practices. Stronger, more adaptable standards are included in version 4.0 to better safeguard cardholder data and respond to changing security threats. Organizations may guarantee they adhere to current security requirements, prevent potential vulnerabilities and preserve the confidence of their partners and customers by updating to the most recent version.

We will be updating to 4.2 compliance on April 1st and recommend that you do the same. To achieve PCI compliance, you need to use TLS 1.2 or higher, with TLS 1.3 being the recommended and more secure option. TLS 1.2 or above must be used when transmitting cardholder data over open, public networks in accordance with PCI DSS version 4.2. This is to guarantee that data is securely encrypted while in transit and shield it from hostile actors'

interception or manipulation. The usage of TLS 1.2 is essential for protecting sensitive credit card data since it is thought to be a more secure protocol than previous iterations.

For Windows licences TLS 1.2 is supported as of PxPlus 2017, version 14, or higher. On UNIX/Linux it requires PxPlus 2017, version 14 or higher, but also depends on the version of OpenSSL that comes with the operating system. If the operating system comes with OpenSSL v1.0.1+ then it will be supported.

For TLS 1.3 our Windows licences require PxPlus 2020, version 17 or higher. On UNIX/Linux PxPlus 2020, version 17, or higher is required and OpenSSL 1.1.1 or higher.

We highly recommend that our clients upgrade to TLS 1.3.

The Payment Card Industry Data Security Standard (PCI DSS) requires the use of secure protocols like TLS to protect cardholder data during transmission. TLS 1.2 is the minimum version required for all HTTPS connections to ensure PCI DSS compliance. TLS 1.3 is recommended due to its enhanced security and performance benefits. Older versions, TLS 1.0 and 1.1, are considered insecure and should not be used for PCI DSS compliance. PCI DSS emphasizes strong cryptography, and both TLS 1.2 and TLS 1.3 provide stronger encryption algorithms than earlier versions. Industry references like NIST SP 800-52 offer guidance on configuring TLS to meet strong cryptography standards.