

PCI DSS Compliance at a Glance

1

WHAT IS PCI DSS COMPLIANCE?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of data security regulations designed to ensure the safe processing, transmission, and/or storage of cardholders' data during payment transactions. Developed in 2004 by the PCI Security Council, it helps protect sensitive payment card information across various industries.

2

WHO NEEDS TO COMPLY?

Organizations that handle payment card information must comply with PCI DSS, which includes:

- Businesses and merchants accepting payments
- Financial institutions such as banks and insurance companies
- Service providers like data centers, payment gateways, and call centers
- E-commerce platforms, online retailers, and SaaS providers

3

KEY PILLARS OF PCI DSS

PCI DSS focuses on six key goals to secure cardholder data:

- Build and maintain a secure network
- Protect cardholder data
- Use regularly updated data security software
- Restricted access to customer data
- Regularly monitor network
- Maintain a documented security policy

4

BENEFITS OF PCI DSS COMPLIANCE

- Build customer trust by showing commitment to data protection.
- Boost your brand reputation by meeting industry standards.
- Foster customer loyalty by keeping their data safe.
- Achieve global compliance with international security standards.
- Strengthen your security systems and reduce potential risks.
- Prevent fraud and data breaches with robust security measures.

5

CONSEQUENCES OF FAILING PCI DSS COMPLIANCE

- Face hefty fines for not complying with PCI DSS standards.
- Risk legal action due to security breaches or negligence.
- Damage your brand's reputation by failing to protect customer data.
- Lose revenue from decreased customer trust and sales.
- Risk losing customers to competitors who follow security standards.
- Increase the chances of data breaches and cyberattacks.