HOMEBASE GUIDE

PCI DSS COMPLIANCE CHECKLIST

What is PCI DSS Compliance?

PCI DSS compliance is a set of requirements outlined by the Payment Card Industry Data Security Standard (PCI DSS). It's intended to ensure that all companies who process, store, or transmit credit card information do so in a secure environment that's protected from bad actors—aka hackers.

Am I already PCI DSS Compliant?

If you're using a payment facilitator, POS, or payment processing platform like Shopify, Square, or any other major tool, you're likely already PCI compliant. Consult your licensing agreement with those vendors if you're unsure, or reach out to your account manager to confirm.

If you're not PCI DSS compliant, follow these steps:

□ Step 1: Determine your PCI DSS compliance level

- **PCI compliance level 1.** The highest compliance level. This is for companies who process more than 6 million transactions per year. This includes all payment facilitators that process more than 300,000 transactions per year.
- **PCI compliance level 2.** This is for companies that process 1–6 million transactions per year. It includes payment facilitators that process fewer than 300,000 transactions per year.
- **PCI compliance level 3**. This is for small businesses who process between 20,000 and 1 million transactions per year.
- **PCI compliance level 4**. The lowest compliance level. This is for companies that process fewer than 20,000 transactions per year.

Step 2:
Work through the 12 PCI DSS compliance requirements

□ **Install and maintain a secure network:** Use firewalls; allow only trusted traffic.

□ **Apply secure configurations through your system:** Set character length and type requirements; enable two-factor authentication (2FA); prompt regular password resets.

□ **Protect stored account data:** Use point-to-point encryption, truncation, masking, and hashing; avoid storing unnecessary data; don't send sensitive information through unsecured channels.

□ **Encrypt cardholder data:** Protect data both at rest and in transit.

□ **Protect systems and networks from malicious software:** Install and maintain protection against Trojans, spyware, worms, ransomware, and malicious links.

□ **Maintain secure systems and software:** Apply all patches and updates promptly.

□ **Deploy proper access control:** Set access rules based on roles and responsibilities.

□ **Identify and authenticate users:** Verify identities; use 2FA for system access.

□ **Restrict physical access to cardholder data:** Lock up hard copies and physical drives; secure computers with data access.

□ **Track all access to system components and cardholder data:** Track user activities and data access; use logs during potential breaches.

□ **Test security regularly:** Use tools and processes to stress test security; perform regular audits.

□ **Create secure organizational policies and programs:** Educate employees on security importance; define roles in data protection.

Step 3:
Complete annual compliance assessments and filings

Annual to-dos depend on your PCI DSS compliance level.

PCI compliance level 1

- □ A yearly self-assessment using the the PCI SSC SAQ.
- □ Quarterly vulnerability scans by an approved scanning vendor or vulnerability management program.
- □ Complete and submit an attestation of compliance form.
- □ A Qualified Security Assessor to complete an Annual Report on Compliance and a quarterly network scan and attestation of compliance.

PCI compliance level 2

- □ A yearly self-assessment using the the PCI SSC SAQ.
- □ Quarterly vulnerability scans by an approved scanning vendor.
- □ Complete and submit an attestation of compliance form.

PCI compliance level 3

- □ A yearly self-assessment using the the PCI SSC SAQ.
- □ Quarterly vulnerability scans by an approved scanning vendor.
- □ Complete and submit an attestation of compliance form.

PCI compliance level 4

- □ A yearly self-assessment using the the PCI SSC SAQ.
- □ Quarterly vulnerability scans by an approved scanning vendor.
- □ Complete and submit an attestation of compliance form.