PII TOOLS

PCI DSS v4.0.1 Checklist

Are you PCI-compliant?

Because advances in technology never stop, the Payment Card Industry Data Security Standard, or PCI DSS for short, has to play a constant game of catch-up. This information security standard organized by major credit card companies (Visa, Mastercard, etc.) is meant to force businesses to process, store, and transmit credit card data in a secure environment.

Version four of this regulation (PCI DSS v4.0) went into force on 1 April 2024, putting into effect its many changes compared to earlier versions. And now with the addition of v4.01, companies have even more updates to consider.

Use the following checklist of 10 REQUIREMENTS to ensure you're up to date on PCI DSS v4's biggest changes

- ☑ **Meet new firewall requirements**
  Properly configure your firewall and routers to protect your payment card data environment. Keep your firewall well-maintained and up-to-date by performing periodic vulnerability tests.

- ☑ **Improved cardholder data security**
  Often considered the most important PCI DSS requirement, safeguarding cardholder data should take priority. Do this by enforcing strong security measures (encryption, PAN masking, etc.), creating a PCI-compliant company policy, and documenting your process for creating, storing, and managing cryptographic keys.

- ☑ **Data access restrictions**
  Individuals should only have access to private cardholder data on a need-to-know + business essential basis. Create and implement documented access control policies, recording all users and their access level (key cards, passcodes, biometrics, etc.).

- ☑ **Upgrade vendor default settings**
  The password, username, and other default security settings for any servers, network devices, or software applications are often insufficient to meet PCI standards. Make sure to upgrade your settings for all new devices and hardware and keep a documented record of everything.

About PII TOOLS

PII Tools is data discovery software that lets you analyze and remediate personal and sensitive data at scale. PII Tools is best used for Audits & Compliance, Breach Management, and Data Migrations. For a product demo, please contact us at info@pii-tools.com.

PCI DSS v4.0.1 Checklist

- [x] **Encrypt data-in-motion**
All cardholder data must be protected using encryption not only while in storage but also transmission. Implement strong encryption protocols in private and public networks and adhere to the PCI DSS measures on Multi-Factor Authentication (MFA)

- [x] **Always secure hardware and software**
Perform a thorough risk assessment of any tech or software before implementation, always keep them up to date, and if you choose to develop your own software, make sure they too are PCI DSS v4.1 compliant.

- [x] **Unique user IDs and passwords**
Every user must have their own unique, individual username and password access, and all group IDs or passwords are now fully forbidden. Be sure to document your processes for creating, assigning, and revoking user IDs and add Two-Factor Authentication (2FA) to your login system.

- [x] **Monitor and document network access**
PCI DSS standards require all network systems to be protected and monitored at all times, with a clear history of all activities (network activity logs). Set up automatically generated audit trails for network documentation and regularly review anything suspicious or out of place.

- [x] **Updated antivirus software**
All hardware and software require antivirus software that performs continuous monitoring and automatically generates records. Don't forget to configure this software so that users can't make unapproved changes to the settings.

- [x] **Keep physical access points under lock and key**
Deploy cameras, CCTV security, or other surveillance in and around any areas with physical access to data protected under this regulation. Use badges and name tags to identify personnel from visitors and liquidate all physical data storage devices when no longer needed.

About PII TOOLS

PII Tools is data discovery software that lets you analyze and remediate personal and sensitive data at scale. PII Tools is best used for Audits & Compliance, Breach Management, and Data Migrations. For a product demo, please contact us at info@pii-tools.com.