

PCI DSS Basic Compliance Guide



**Interactive
Content**

- 1. What does PCI mean?**
- 2. Why do we need to comply with PCI DSS and what are the consequences of non-compliance?**
- 3. What steps do I need to take to comply with PCI?**

Breaching the privacy of your customers' payment cards has a direct effect on your business: reputational damage, loss of trust, fines and penalties, and many other consequences that could harm your company. The number of configurations and functionalities for payment methods is increasing. If not used properly, they can become a weak point facilitating access to customer data. For example, Wi-Fi technology, remote access software or recording systems, among others.

This is why it is important to consider some basic concepts to ensure you comply with the obligatory security obligations that apply to all merchants. Below, we list the basic concepts.

1 | What does PCI mean?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that all merchants or service providers that process or store card data must comply with. They provide a **set of technical and operational requirements intended to protect cardholder data**.

The PCI Security Standards Council, which was created by leading international payment brands, is responsible for establishing these security standards, which apply to everyone involved the sector (financial institutions, businesses, service providers, software companies, etc.).

2 | Why do we need to comply with PCI DSS and what are the consequences of non-compliance?

Compliance is necessary in order to ensure we fully protect our customers' card data. It helps to know that:

- **Protecting data** helps us prevent fraud associated with security breaches that may occur in the system, as well as "data compromises". In other words, any illegal access to cardholder data.
- **We should avoid losing our customers'** trust. Customers assume that their card details are safe at all times and in any system.
- **There may be damage to the brand**, the acquirer and, to a greater extent, the merchant if data is accessed illegally, which may have economic, image or reputational consequences, which would jeopardise the merchant's business.
- **The techniques used by criminal organisations get better** over time and they find more and more ways to access merchants' systems. Therefore, it is important to comply with the technical and security requirements to prevent intrusions.

What happens if the merchant does not comply with the PCI DSS standards? Non-compliance can lead to serious consequences, for example:



Payment of fines or penalties imposed by payment brands or even by acquirers, as well as the potential payment of compensation to affected customers, since cardholders will never be liable for any charges made and not recognised as their own. There could also be other costs such as for forensic investigations (PFI) or corrective actions (since corrective actions more expensive than preventive actions).



It may no longer be possible to work with the acquirer since the acquirer has to guarantee that all acquired merchants comply with said standards so as to prevent reputational risk, economic risk or the risk of fines and penalties.




Other laws and regulations may also be breached.

3 | What steps do I need to take to comply with PCI?

To protect our customers' data, it is necessary to:


- 1. Develop and maintain a secure network.**
- 2. Protect stored cardholder data**, encrypt data and other sensitive information sent over open public networks.
- 3. Maintain a vulnerability management programme** (use and maintenance of antivirus and secure applications).
- 4. Implement strong access control measures** (access restrictions, unique IDs).
- 5. Regularly monitor and test networks.**
- 6. Maintain an information security policy.**

The good news is you can start protecting your business today with these basic security tips:



Use strong passwords and change default passwords

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>



Protect card data and only store what you need

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 75%;"><div style="background-color: red; height: 5px;"></div></div>




Check payment terminals for any signs of tampering

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 75%;"><div style="background-color: red; height: 5px;"></div></div>




Use trusted business partners and find out how to contact them

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>



Install patches from your vendors

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>




Protect internal access to card data

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 75%;"><div style="background-color: red; height: 5px;"></div></div>




Do not make it easy for hackers to access your systems

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>



Use antivirus software

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 75%;"><div style="background-color: red; height: 5px;"></div></div>



Scan for vulnerabilities and fix problems

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>



Use secure payment terminals and software

Value	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>



Protect your business online

Value	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 50%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>



For optimal protection, make your data useless to criminals

Value	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>
Easy payment	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>
Risk mitigation	<div style="width: 100%;"><div style="background-color: red; height: 5px;"></div></div>

In addition to the above, depending on the PCI level held by the merchant, there will be other obligations, such as the submission of various documents and the performance of audits. These are explained briefly below:

What PCI level do I have as a merchant?

To comply with all security requirements, there are different PCI levels for merchants. Merchants are assigned a series of documents depending on their level, which are required by payment brands in order to validate the compliance level.

Nível 1: EstabeleceLevel 1: Merchants that process more than six million transactions per year (documents: ROC, AOC and ASV).

Level 2: Merchants that process between one and six million transactions per year (documents: SAQ, AOC and AV).

Level 3: Merchants that process between 20,000 and one million annual e-commerce transactions (documents: SAQ and AOQ)

Level 4: E-commerce merchants that process less than 20,000 transactions and other merchants that process less than one million transactions (document: SAC)

What is each document for?

- **ROC** (Report on Compliance): A report certifying compliance with PCI standards. A level-1 merchant PCI DSS audit can either be carried out by a qualified external (QSA) or internal (ISA) assessor. For service providers, the audit can only be carried out by an external assessor.
- **SAQ** (self-assessment questionnaire): self-assessment document for merchants and service providers, which records the degree of PCI DSS compliance. Different controls will be performed depending on the merchant type.
- **AOC** (Attestation of Compliance): a declaration of compliance containing a simplified version of the SAQ or the ROC.
- **Scans by an ASV** (Approved Scanning Vendor): Internal and external scans of network vulnerabilities on a quarterly basis carried out by a company approved by the PCI SSC as an ASV.