STANDARD SUMMARY · CERT.GT

PCI DSS

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: Merchants, processors, banks and service providers that handle card data.

PCI DSS is the security standard for anyone who stores, processes or transmits payment card data. It is not a law: the card brands require it through the acquiring banks, by contract. The current version is 4.0.1.

The essentials

- It applies if you accept cards, even with a single card terminal or a payment button on your website.
- Version 3.2.1 was retired on March 31, 2024. The new requirements in version 4 have been mandatory since March 31, 2025.
- The best way to comply is to reduce the scope: the fewer systems that handle card data, the less there is to protect and audit.
- Never store the security code (CVV), the PIN or the magnetic stripe after authorization, not even encrypted.

The 12 requirements

1	Install and maintain network security controls.
2	Apply secure configurations to all system components.
3	Protect stored account data.
4	Protect cardholder data with strong cryptography during transmission over public networks.
5	Protect all systems and networks from malicious software.
6	Develop and maintain secure systems and software.
7	Restrict access to data by business need to know.
8	Identify users and authenticate access.
9	Restrict physical access to cardholder data.
10	Log and monitor all access to systems and data.
11	Test security of systems and networks regularly.
12	Support information security with organizational policies and programs.

What is new in version 4

- Two-step verification for all access to the cardholder data environment, not just for administrators.
- Passwords of at least 12 characters.
- Control over the scripts that payment pages load, and detection of unauthorized changes to those pages.
- Technical protection against phishing and automated log review.
- The “customized approach” option: meeting the objective of a requirement with a different control, if it is shown to work.
- Targeted risk analysis to define how often several periodic activities are performed.

How it is validated

- The merchant level depends on the number of transactions per year and is defined by each brand; your acquiring bank tells you which one applies to you.
- Small merchants fill out a Self-Assessment Questionnaire (SAQ); there are several types depending on how you accept cards.
- The highest levels require an on-site audit by a Qualified Security Assessor (QSA) and a Report on Compliance (ROC).
- If you have systems exposed to the internet, quarterly scans by an Approved Scanning Vendor (ASV) are required.

How to reduce the scope

- Use a payment gateway or payment page hosted by the processor: that way card data does not pass through your servers.
- Use terminals with validated point-to-point encryption (P2PE).
- Replace the card number with a token if you need to make recurring charges.
- Separate, on the network, the systems that handle cards from the rest of the company.

Common mistakes

- Storing card numbers in spreadsheets, emails or call recordings.
- Believing that outsourcing payments removes all responsibility: you still answer for your part of the process.
- Complying once a year for the audit and not maintaining the controls the rest of the time.

Official text

PCI DSS v4.0.1, from the PCI Security Standards Council, free at pcisecuritystandards.org.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

Summary prepared by cert.gt for educational purposes; it is not the official text of the standard and does not replace legal or compliance advice. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).