WORLDLINE

Payments to grow your world

PCI DSS compliance instructions Security standards for merchants.

All merchants worldwide that transmit, process or store card data are required to comply with the security guidelines defined in the Payment Card Industry Data Security Standard (PCI DSS). If these guidelines are not observed, Worldline is entitled to terminate the contractual relationship with immediate effect and to claim compensation for any claims or penalties incurred.

The following instructions, in the form of technical and organizational guidelines, represent binding components of every contract with Worldline.

What does PCI DSS cover?

PCI DSS encompasses 12 mandatory requirements aimed at protecting card data during processing, storage and transmission. PCI DSS is implemented through the security programs of the card organizations. These include AIS from Visa, SDP from Mastercard and the equivalent programs from American Express, Discover (Diners Club) and JCB.

Why was PCI DSS introduced?

The theft of card data has steadily increased in recent years. The fraudulent use of stolen card data has caused significant losses for all parties involved.

What is the purpose of PCI DSS?

With PCI DSS, the card organizations seek to further enhance the security of card payments to protect merchants and cardholders, as well as the industry as a whole, more effectively against the theft and misuse of card data.

Who is required to comply with PCI DSS?

PCI DSS requires all merchants worldwide that transmit, process or store card data to take and maintain effective security measures.

Furthermore, the merchants are responsible for ensuring that any third parties they engage which could impact on the security of card holder data or perform activity on behalf of the merchant, such as web hosting companies or payment service providers (PSPs) also comply with PCI DSS.

See also the sections related to “data protection” and “liability” of the general business conditions applicable to the card acceptance.

Who is responsible for compliance with PCI DSS?

It is fundamentally each merchant’s responsibility to comply with the PCI DSS security guidelines. However, the card organizations also require merchants to declare (have themselves certified) the security measures they have implemented. The scope of declaration (certification) depends on the number of transactions conducted.

What types of certification methods are there?

- **Self-Assessment Questionnaire (SAQ)**
  This involves completing a self-assessment questionnaire.
- **On-Site Audit**
  Merchants with large transaction volumes and possibly those that have been the victim of card data theft are obliged to complete a report on compliance (ROC).
  The report and attestation must be performed by a qualified security assessor (QSA) or internal security assessor (ISA).
- **Network Scan**
  An accredited certification firm (approved scanning vendor) carries out a targeted scan on a quarterly basis, in coordination with the merchant, to identify possible vulnerabilities.

If the merchant fails to fully meet all the certification criteria, then they are required to improve the security arrangements in the relevant areas immediately and maybe subject to financial penalties until compliance is attained.

Who bears the expenses for certification?

The costs for the certification measures are to be covered in full by the merchant, as are the costs for rectifying deficiencies identified during the certification process.

What happens if a merchant does not obtain certification?

If a merchant who is required to obtain certification fails to do so, then Worldline is entitled to terminate the contractual relationship with immediate effect and to claim penalties charged by the card organizations and compensation for losses claimed by the card issuer.

Who can view the certification data?

Only the merchant and the certification company can view the data collected in the scope of the certification process. However, the merchant is required to submit a summary of the certification results to Worldline, which is also entitled to view the self-assessment questionnaires. The card organizations, on the other hand, only receive statistical evaluations.

How often must certification be renewed?

All Entities must undergo annual assessment and entities with internet facing IP addresses (e-commerce etc.) must also undergo quarterly ASV (vulnerability) scans.
Any significant changes to the merchant environment must be reported to Worldline immediately in order to assess whether these impact on the commercial or compliance requirements.

Through which companies must the certification measures be conducted?

You will find a list of all accredited certification firms on the Internet:

- for the conducting of on-site audits:
  pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- for the conducting of network scans:
  pcisecuritystandards.org/pdfs/asv_report.html

Where can I learn more about PCI DSS?

You can find further information about PCI DSS at the following websites:

- Worldline: worldline.com/merchant-services/pci
- PCI Security Standards Council: pcisecuritystandards.org

Your local point of contact can be found at: worldline.com/merchant-services/contacts

110.00110.02 INT_EN/08.2023