Payment Services

# PCI DSS compliance instructions Security standards for merchants

**All merchants worldwide who transmit, process or store card data are obliged to comply with the security guidelines defined in the Payment Card Industry Data Security Standard (PCI DSS). If these regulations are not observed, SIX Payment Services is entitled to terminate the contractual relationship without notice and claim compensation of damages or any penalties incurred.**

**The following instructions in the form of technical and organisational guidelines represent binding elements of every contract with SIX Payment Services.**

## Why has PCI DSS been introduced?

Instances of card data theft have increased massively over the last few years. The fraudulent use of the stolen card data has given rise to immense damages for all parties involved.

## What is the purpose of PCI DSS?

The card organisations have devised PCI DSS as a means of increasing 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.

## What does PCI DSS cover?

PCI DSS encompasses 12 compulsory requirements aimed at protecting card data during processing, storage and transmission. PCI DSS is being implemented under the security programmes of the card organisations. These include AIS from Visa, SDP from MasterCard and the equivalent programmes from American Express, Discover (Diners Club) and JCB.

## Who is obliged to comply with PCI DSS?

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

Furthermore, the merchants are responsible for ensuring that third parties they engage to transmit, process or store data on their behalf, such as payment service providers (PSPs) or data storage entities (DSEs), also comply with PCI DSS.
See also:
– Paragraph 13 of the "General business conditions for cashless payments"

## Who is responsible for compliance with PCI DSS?

It is the merchant's responsibility to comply with PCI DSS. However, the card organisations also require the merchants to declare (certify) the security measures they have implemented. The scope of certification depends on the number of transactions conducted and whether the merchant is involved in the transmission, processing or storage of card data.

## What certification methods are there?

PCI DSS distinguishes between the following three methods (see also the table overleaf):

– **Self-Assessment Questionnaire (SAQ)**
  This involves completing a self-assessment questionnaire.
– **Network Scan**
  An accredited certification company (approved scanning vendor) carries out a friendly hacker attack on a quarterly basis, as agreed with the merchant, in order to identify possible vulnerabilities.
– **On-Site Audit**
  Merchants with large transaction volumes, merchants who have had a data compromise, and all payment service providers and other service providers that transmit, store or process card data on behalf of third parties are inspected on site. Whereas merchants may have such an audit conducted internally by a specially trained auditor and signed off by a company manager, service providers must be audited by an accredited certification company (qualified security assessor).

If the merchant fails to fully meet all the certification criteria, he is obliged to improve the security arrangements in the relevant areas immediately.

## Who bears the expenses for certification?

The cost of the certification is covered in full by the merchant or mandated third party, as is the cost of rectifying deficiencies identified during the certification process.

## What happens if a merchant does not obtain certification?

If a merchant who is obliged to obtain certification fails to do so, SIX Payment Services is entitled to terminate the contractual relationship without notice and to claim penalties charged by the card organisations and compensation for damages asserted by the card issuers.

## Who can access the certification data?

Only the merchant and the certification company can access the data collected as part of the certification process. However, the merchant is obligedto submit a summary of the certification results to SIX Payment Services. SIX Payment Services similarly has access to the self-assessment questionnaires. The card organisations, on the other hand, only receive statistical evaluations in encrypted form.

## How often must certification be renewed?

The certification must be repeated on a regular basis, as shown in the table below:
changes on the merchant side, such as the installation of new hardware or software, a new website or a change of service provider, must be reported to SIX Payment Services immediately. In some circumstances, this may make it necessary to obtain a new certification.

## Which entities are permitted to carry out certifications?

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

- for the execution of onsite audits (Level 1 merchants): www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- for the execution of network scans: www.pcisecuritystandards.org/pdfs/asv_report.html

## Where can I find out more about PCI DSS?

You will find more information about PCI DSS on the PCI Security Standards Council website: www.pcisecuritystandards.org

## Who needs to take which certification measures?

| Level | Description | Visa MasterCard/ Maestro Diners/ Discover | JCB | American Express |
|---|---|---|---|---|
| 1 | Merchants with more than 6 million transactions per year | – Annual Network Scan<br>– Quarterly On-Site Audit | | |
| | Merchants after esuffering previous hacker attack with card data fraud | | | |
| | Merchants with more than 2.5 million transactions per year | | | – Annual On-Site Audit<br>– Quarterly Network Scan |
| | Merchants with more than 1 million transactions per year | | – Annual On-Site Audit<br>– Quarterly Network Scan | |
| 2 | Merchants with 1–6 million transactions per year | – Quarterly Network Scan<br>– Annual Self-Assessment Questionnaire | | |
| | Merchants with 50,000–2.5 million transactions per year | | | – Quarterly Network Scan |
| 3 | E-commerce merchants with 20,000–1 million transactions per year | – Quarterly Network Scan<br>– Annual Self-Assessment Questionnaire | | |
| | Merchants with fewer than 50,000 transactions per year | | | – Quarterly Network Scan |
| 4 | E-commerce merchants with fewer than 20,000 transactions per year | – Quarterly Network Scan<br>– Annual Self-Assessment Questionnaire | – Quarterly Network Scan<br>– Annual Self-Assessment Questionnaire | |
| | Merchants (excluding e-commerce) with fewer than 1 million transactions per year | | | |

On-site audits and/or network scans are mandatory only for merchants that process, transmit or store cardholder data electronically. However, we do recommend these validation methods anyway, especially for merchants with complex system infrastructures.

110.0157.02 INT_EN/04.2012

Your personal contact: www.six-payment-services.com/contact

**SIX Payment Services Ltd**
Hardturmstrasse 201
8005 Zurich
Switzerland

**SIX Payment Services (Europe) S.A.**
10, rue Gabriel Lippmann
5365 Munsbach
Luxembourg