

Instructions for merchants concerning compliance with the PCI security regulations

All merchants worldwide who transmit, process or store card data are obligated to adhere to the Payment Card Industry Data Security Standard (PCI DSS) defined security guidelines. If these regulations are not observed, Telekurs Multipay is entitled to terminate the contractual relationship without notice and claim damages for any penalties or debts incurred.

The following instructions in the form of technical and organisational guidelines represent binding components of every contract with Telekurs Multipay.

Why has PCI been introduced?

Hacker attacks on computer systems have increased over the last few years, with huge quantities of card data being stolen in some cases. This has given rise to immense damages for all parties involved.

What is the purpose of PCI?

The card organisations aim to further increase the security of card-based payments with PCI to protect merchants and cardholders alike even more effectively against data theft and misuse.

What does PCI cover?

PCI encompasses the data-security programs of all major card organisations. This includes SDP (Site Data Protection) from MasterCard, AIS (Account Information Security) from Visa and the equivalent programs from American Express and JCB.

Who is required to comply with PCI?

PCI requires all merchants throughout the world who transmit, process or store card data to take and maintain effective security measures.

The merchants are also 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 the security guidelines.

Please see:

- Paragraph 14.1 of the “General business conditions for cashless payments”
- Paragraph 12.4 of the “Special business conditions for the acceptance of credit cards in the absence of the card”
- Paragraph 12.4 of the “Special business conditions for the acceptance of debit cards in the absence of the card”

Who is responsible for compliance with PCI?

It is normally the personal responsibility of each and every merchant to comply with the security regulations. However, the card organisations require the merchants to have the security measures they have implemented to be certified. Whether and to what extent certification is necessary depends on the number of transactions handled by the merchant.

What types of certification are there?

The card organisations distinguish the following three types of certification (see also the table overleaf):

- **Self Assessment Questionnaire (SAQ)**

A detailed security questionnaire must be completed.

- **Network Scan**

A security firm (approved scanning vendors) accredited by Visa and/or MasterCard carries out a friendly hacker attack on a periodic basis, as agreed with the merchant, in order to identify possible weaknesses.

- **On-Site Security Audit**

Large or critical merchants in terms of security, together with all payment service providers and other service providers, are inspected on site. While merchants can carry out such an audit themselves, or can have it conducted by a trained auditor and have it certified by a person in charge of business operations, payment service providers are required to be audited by an accredited security firm (qualified security assessors).

If the merchant fails to satisfy the certification criteria in full, he is required to improve his security arrangements in the relevant areas.

Who covers the cost of certification?

The cost of 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 required to obtain certification fails to do so, Telekurs Multipay is entitled to terminate the contractual relationship without notice and to claim damages for any penalties charged by the card organizations and claims asserted by the card issuer.

Who can access the certification data?

Only the certified company and the security firm can access the data collected as part of the certification process. The merchant is obliged, however, to send a copy of the certification results to Telekurs Multipay. The card organizations, on the other hand, only receive statistical evaluations or summaries in encrypted form.

How often must certification be renewed?

The certification must be renewed at regular intervals:

- Network Scans: 4x/year
- On-Site Security Audits: 1x/year
- Self Assessment Questionnaire 1x/year

Telekurs Multipay must also be immediately notified should changes occur at the merchant, such as the installation of new hardware or software, a new Web site or a switching of service providers. Depending on the circumstances, a recertification may be necessary.

Which security firms are permitted to carry out certifications?

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

- For On-site security audits (customer level 1):
www.visaeurope.com/documents/ais/qualified_security_assessors.pdf – Qualified Security Assessors (QSAs)
- For the execution of network scans:
www.pcisecuritystandards.org/resources/approved_scanning_vendors.htm – Approved Scanning Vendors (ASVs)

Where can I find out more about PCI?

You will find more information on PCI on the websites of the card organizations:

- MasterCard:
www.mastercard.com/us/sdp/merchants/merchant_levels.html
- Visa:
www.visaeurope.com/aboutvisa/security/ais/resourcesanddownloads.jsp
- American Express:
[www209.americanexpress.com/merchant/singlevoice/dsw/
FrontServlet?request_type=dsw&pg_nm=home&ln=en&frm=GB](http://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home&ln=en&frm=GB)
- and directly from the PCI Security Standards Council:
www.pcisecuritystandards.org/about/faqs.htm



Who requires certification?

Level	Description	Visa	MasterCard/ Maestro	JCB	American Express
1	Merchants with more than 6 million transactions per year	<ul style="list-style-type: none"> • Annual On-Site Security Audit • Quarterly Network Scan 			
	Merchants with past hacker attacks and/or data misuse				
	Merchants with more than 2.5 million transactions per year				<ul style="list-style-type: none"> • Annual On-Site Security Audit • Quarterly Network Scan
	Merchants with more than 1 million transactions per year			<ul style="list-style-type: none"> • Annual On-Site Security Audit • Quarterly Network Scan 	
2	Merchants with 1-6 million transactions	<ul style="list-style-type: none"> • Quarterly Network Scan • Annual Self Assessment Questionnaire 			
	Merchants with 50,000-2.5 million transactions per year				<ul style="list-style-type: none"> • Quarterly Network Scan
3	E-commerce merchants with 20,000-1 million transactions per year	<ul style="list-style-type: none"> • Quarterly Network Scan • Annual Self Assessment Questionnaire 			
	Merchants with fewer than 50,000 transactions per year				Recommended: <ul style="list-style-type: none"> • Quarterly Network Scan
4	E-commerce merchants with fewer than 20,000 transactions per year	Recommended: <ul style="list-style-type: none"> • Quarterly Network Scan • Annual Self Assessment Questionnaire 		<ul style="list-style-type: none"> • Annual Self Assessment Questionnaire • Quarterly Network Scan 	
	Merchants (excluding e-commerce) with fewer than 1 million transactions per year				

The On-Site Security Audit or the Network Scan are recommended for customers who do not process, transmit or store card data.