



These “Instructions for adherence to the SDP/AIS security rules for merchants” are a binding component of the contractual relationship to Telekurs Multipay, serving as technical and organizational instructions. They are therefore to be read and adhered to by the merchant (see section 14.1 of the General Business Conditions for Cashless Payments and section 12.4 of the Special Business Conditions for the Acceptance of Credit Cards in the Absence of the Card), as well as the Special Business Conditions for the Acceptance of Debit Cards in the Absence of the Card). Failure to adhere to these regulations represents a contract infraction by the merchant and could result in legal repercussions as established in the General and Special Business Conditions. Specifically, they entitle Telekurs Multipay to immediately terminate the contract relationship and to assert claims for damages as a result of fines levied by the card organizations and claims for compensation from the card issuer.

Adherence to the security requirements in accordance with the programs SDP (Site Data Protection) from MasterCard and AIS (Account Information Security) from VISA is mandatory worldwide for all merchants that transmit, process and store credit card or debit card data.

Initial position

The number of cases in which unauthorized persons have infiltrated IT systems has increased in recent years, leading in some cases to data from millions of cards landing in the wrong hands to be used for fraudulent purposes. Considerable losses have thus been incurred by all participants. This threat should be countered and enhanced security provided with the programs SDP and AIS which contain all security standards stipulated by the card organizations for card payments over the Internet (Payment Card Industry – PCI – security standards).

Who is obligated to adhere to the security requirements according to SDP/AIS?

All merchants that transmit, process or store card data are obligated to adhere to the security rules according to SDP/AIS. The merchants are responsible for ensuring that their assigned third parties that transmit, process or store card data also adhere to these rules.

How is adherence to SDP/AIS validated?

Differentiation is made between the **obligation** to adhere to the security rule and the **proof** of such adherence by means of a **certification**. The rules are determined by the size of the merchant. The following applies:

Allocation of the merchant according to the number of transactions per merchant, per card system and per year	Actions to be taken
Fewer than 20,000 e-commerce transactions per year and card system (and less than 6,000,000 transactions per year and card system in all channels including presence business)	<p>Recommendation</p> <p>Annual completion of the security questionnaire by the merchant; 1 security scan each year by an accredited security firm</p>
Between 20,000 and 6,000,000 e-commerce transactions per year and in one card system	<p>Requirement: Certification</p> <p>Annual completion of the security questionnaire by the merchant and assessment by an accredited security firm; 4 security scans each year by an accredited security firm</p>
More than 6,000,000 transactions per year and in one card system in all channels (including presence business)	<p>Requirement: Certification</p> <p>On-site security audit by the merchant or an external security firm accredited by the card organizations; 4 security scans each year by an accredited security firm</p>

Please note that special rules apply to assigned third parties. You can consult with security companies and Telekurs Multipay in this regard.



Means of certification

Self Assessment Questionnaire (SAQ)

By completing a detailed SDP/AIS security questionnaire, a merchant can assess how his/her Web service meets the PCI security regulations. All questions must be answered either with «yes» or «not applicable». The purpose of the questionnaire is to encourage the merchant to implement measures that positively modify the security on his/her Web server. If desired, the merchant can also assign the completion of the questionnaire and the solving of any security-related problems to a security firm.

Security Scan

A security firm accredited by MasterCard or VISA will carry out these tests on a regular basis to see whether the merchant's system can withstand known hacker attacks.

On-site security audit

For very large or security-critical merchants, payment service providers and other service providers, a physical inspection (on-site security audit) will be arranged. Merchants can carry out the on-site security audit themselves, however, for payment service providers an accredited security company is required to conduct the audit.

Who bears the costs for the SDP/AIS audits?

The certification costs are borne by the merchant or authorized third party as are the costs required to rectify any problems identified during the certification. Any necessary reexaminations will be made by the selected security firm.

What happens if you do not get certified?

Failure to adhere to the regulations represents a contract infraction by the merchant and could result in legal repercussions as established in the General and Special Business Conditions. Specifically, they entitle Telekurs Multipay to immediately terminate the contract relationship and to assert claims for damages as a result of fines levied by the card organizations and claims for compensation from the card issuer.

Who can view the data that the merchant provides to the security firm within the certification process?

Only the merchant to be certified and the security firm have access to this information. Telekurs Multipay only receives an overall assessment of the merchant from the security firm. As card organizations, MasterCard and VISA receive only statistical evaluations.

Must the SDP/AIS certification be renewed periodically?

Certification is to be renewed annually. Any change of circumstances at the merchant (e.g. new hardware, software, network, Web site as well as a change of payment service provider, Internet service provider or the DSE) must be reported to Telekurs Multipay, even if the merchant is not obligated to be certified. The registration and/or certification may possibly be required to be subsequently renewed.

- Security scans – if necessary – are to be made four times annually
- On-site reviews – if necessary – are to be made annually

Security firms

You can find a directory of accredited security firms at www.visa-europe.com or sdp.mastercardintl.com.

Further information

You can find further information about SDP and AIS on the Web sites of the accredited security firms or at:

- Telekurs Multipay Ltd. www.secure-ecommerce.ch