SWISSCARD PCI DSS AND SECURITY REQUIREMENTS POLICY FOR CONTRACTUAL PARTNERS

General
Swisscard AECS GmbH (Swisscard) has, for many years, been committed to protecting cardholder data in order to ensure maximum security. The unauthorized use of data has a negative impact on cardholders, contractual partners, service providers and card issuers. The introduction of the Payment Card Industry Data Security Standards (PCI DSS), in response to this threat, help strengthen customer confidence, increase profitability and enhance a company's reputation. At Swisscard we know our contractual partners share these concerns and therefore, as part of your responsibility, we require you to comply with the data protection provisions within the Terms and Conditions for Accepting American Express Cards and this policy which we will revise from time to time.

PCI DSS
The Payment Card Industry Data Security Standards (PCI DSS) were developed several years ago by Visa International, MasterCard, American Express, JCB and Discover to promote the global introduction of consistent data security measures and to preventatively protect card data, thereby increasing security when handling card data. They are published by the PCI Security Standards Council and regulate the technical and operational requirements for all parties that save, process and transmit card data.
The latest version of the detailed requirements can be viewed at any time at www.pcisecuritystandards.org.

Responsibilities
The PCI DSS are mandatory for all our contractual partners, banks, processors and payment service providers who save, process or transmit cardholder data for their own purposes or on behalf of other organizations. It is the contractual partner's responsibility to comply with the PCI DSS. Contractual partners will also be responsible for the PCI DSS compliance of any engaged third parties, e.g. payment service providers, who process, save or transmit card data on their behalf. The costs of the certification measures will be borne in full by the contractual partner or engaged third party.

How to proceed
In order to demonstrate PCI DSS compliance, the contractual partner is obliged to document any security measures it has taken (certification measures). The table below shows contractual partners, based on their annual transaction volume, what duties they have and which documents must be submitted in order to evidence PCI DSS compliance.
It is important to note that contractual partners in levels 3 and 4 need only submit certification documents upon Swisscard's request but nevertheless remain liable and subject to all other provisions of the PCI DSS. Swisscard will inform these contractual partners in writing at least ninety (90) days prior to the required submission of documents.

Level/Annual American Express Transactions	On Site Assessment Report on Compliance (ROC)	Self Assessment Questionnnaire (SAQ) AND Quarterly Scan	STEP Attestation for eligible Merchants
Level 1 **2.5 million or more**	Mandatory	Not Applicable	Optional (replaces ROC)
Level 2 **50,000 to 2.5 million**	Optional	SAQ Mandatory (unless submitting On-site Assessment): scan mandatory with certain types of SAQ.	Optional (replaces SAQ and Network scan or ROC)
Level 3 **10,000 to 50,000**	Optional	SAQ optional (Mandatory if required by Swisscard or American Express): scan mandatory with certain types of SAQ.	Optional (replaces SAQ and Network scan or ROC)
Level 4 **10,000 or less**	Optional	SAQ optional (Mandatory if required by Swisscard or American Express): scan mandatory with certain types of SAQ.	Optional (replaces SAQ and Network scan or ROC)

What to do in the case of a data breach?
You must notify Swisscard **immediately, but within twenty four (24) hours at the latest** of discovering the data breach by phone on **044 659 64 44** (24 hour phone service)

For questions and further information
For questions related to PCI please contact our service centre on **044 659 64 44** (24 hour phone service).
For More detailed information please refer to the American Express DSOP (Data Security Operating Policy) available online at www.americanexpress.com.
Please note that documentation submitted must not be submitted directly to American Express but to Swisscard. Please contact us for further details.

Glossary
Annual On Site Security Assessment: The Annual On Site Security Assessment is a detailed on-site security check on your devices, systems and networks (and associated components) used to save, process or transfer cardholder data or confidential authentication data (or both).

Annual Self Assessment Questionnaire: The PCI DSS Self Assessment Questionnaire (SAQ) is used to self test your devices, systems and networks (and associated components) used to save, process or transfer cardholder data or confidential authentication data (or both).

Version 2025/01

2500M/09.2025