SWISSCARD WEISUNG ZUR EINHALTUNG DER PCI DSS SICHERHEITSVORSCHRIFTEN FÜR VERTRAGSPARTNER

Allgemeines
Swisscard AECS GmbH (Swisscard) hat sich schon seit vielen Jahren dem Schutz der Daten seiner Karteninhaber verpflichtet, um höchste Sicherheit zu gewährleisten. Die unberechtigte Nutzung von Daten wirkt sich negativ auf Karteninhaber, Vertragspartner, Dienstleister und Kartenherausgeber aus. Die Einführung der Payment Card Industry Data Security Standards (PCI DSS) als Antwort auf diese Bedrohung trägt dazu bei, das Vertrauen der Kunden zu stärken, die Rentabilität zu steigern und die Reputation eines Unternehmens zu erhöhen. Bei Swisscard wissen wir, dass Vertragspartner unser Anliegen teilen. Wir setzen daher als Teil Ihrer Verantwortung voraus, dass Sie die Datenschutzbestimmungen der Bedingungen für die Akzeptanz von American Express Karten und diese Richtlinie, die wir von Zeit zu Zeit überarbeiten, einhalten.

PCI DSS
Die Payment Card Industry Data Security Standards (PCI DSS) wurden bereits vor einigen Jahren von Visa International, MasterCard, American Express, JCB und Discover entwickelt, um die weltweite Einführung konsistenter Datensicherheitsmassnahmen zu unterstützen und Kartendaten präventiv zu schützen und damit die Sicherheit beim Umgang mit Kartendaten zu erhöhen. Sie werden vom PCI Security Standards Council publiziert und regeln die technischen und betrieblichen Anforderungen für alle Parteien, die Kartendaten speichern, verarbeiten oder übermitteln. Die detaillierten Anforderungen der jeweils gültigen Fassung sind jederzeit unter www.pcisecuritystandards.org einsehbar.

Verantwortlichkeiten
PCI DSS ist verpflichtend für alle unsere Vertragspartner, Banken, Datenauftragsverarbeiter und Payment Service Provider, die Karteninhaberdaten für eigene Zwecke oder im Namen anderer Organisationen speichern, verarbeiten oder übermitteln. Es liegt in der Eigenverantwortung der Vertragspartner, die PCI DSS einzuhalten. Vertragspartner sind auch für die Einhaltung der PCI DSS durch beigezogene Dritte, z.B. Payment Service Provider, die in ihrem Namen Kartendaten verarbeiten, speichern oder übermitteln, verantwortlich. Die Kosten für die Zertifizierungsmassnahmen gehen vollumfänglich zu Lasten des Vertragspartners bzw. des beigezogenen Dritten.

Wie geht der Vertragspartner vor
Um die Einhaltung der PCI DSS nachzuweisen, ist der Vertragspartner verpflichtet, die von ihm getroffenen Sicherheitsmassnahmen zu dokumentieren (Zertifizierungsmassnahmen). In der nachstehenden Tabelle finden Vertragspartner basierend auf ihrem jährlichen Transaktionsvolumen, welche Pflichten sie haben und welche Dokumente eingereicht werden müssen, um die Einhaltung der PCI DSS nachzuweisen.
Bitte beachten Sie, dass Vertragspartner der Stufen 3 und 4 nur auf Verlangen von Swisscard Zertifizierungsdokumente einreichen müssen, aber dennoch der Haftung und allen anderen Bestimmungen der PCI DSS unterliegen. Swisscard informiert diese Vertragspartner schriftlich mindestens neunzig (90) Tage vor der erforderlichen Einreichung der Dokumente.

Stufe/jährliche American Express Transactions	Bericht über das «Annual Onsite Security Assessment» (Report on Compliance, ROC)	Fragebogen «Self Assessment Questionnaire» (SAQ) UND vierteljährlicher Scan	STEP-Nachweis für qualifizierte Händler
Stufe 1 **2.5 Millionen oder mehr**	Obligatorisch	Nicht anwendbar	Optional (ersetzt ROC)
Stufe 2 **50 000 bis 2.5 Millionen**	Optional	SAQ obligatorisch (ausser bei Einreichung von On Site Assessment): Scan obligatorisch mit bestimmten Arten von SAQ.	Optional (ersetzt SAQ und Netzwerkscan oder ROC)
Stufe 3 **10 000 bis 50 000**	Optional	SAQ optional (obligatorisch auf Verlangen von Swisscard oder American Express): Scan obligatorisch mit bestimmten Arten von SAQ.	Optional (ersetzt SAQ und Netzwerkscan oder ROC)
Stufe 4 **10 000 oder weniger**	Optional	SAQ optional (obligatorisch auf Verlangen von Swisscard oder American Express): Scan obligatorisch mit bestimmten Arten von SAQ.	Optional (ersetzt SAQ und Netzwerkscan oder ROC)

Vorgehen bei einem Datenvorfall
Sie müssen Swisscard **unverzüglich, spätestens jedoch innerhalb von vierundzwanzig (24) Stunden** nach der Entdeckung eines Datenvorfalls, telefonisch benachrichtigen unter **044 659 64 44** (24-Stunden-Telefonservice)

Fragen und weitere Informationen
Bei Fragen zur PCI steht Ihnen unser Servicecenter unter der Nummer **044 659 64 44** (24-Stunden-Telefonservice) zur Verfügung.
Weitere Informationen finden Sie in der American Express DSOP (Data Security Operating Policy, Allgemeine Datensicherheitsrichtlinien), die online unter www.americanexpress.com verfügbar sind. Bitte beachten Sie, dass die Dokumentation nicht direkt American Express, sondern Swisscard vorgelegt werden muss. Für weitere Details stehen wir Ihnen gerne zur Verfügung.

Glossar
Annual On Site Security Assessment: Beim Annual On Site Security Assessment handelt es sich um eine detaillierte Vor-Ort-Sicherheitsprüfung Ihrer Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), mit denen Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder beides) gespeichert, verarbeitet oder übertragen werden.

Annual Self Assessment Questionnaire: Bei der jährlichen Selbsteinschätzung dient der PCI DSS Fragebogen «Self Assessment Questionnaire» (SAQ) der Selbstprüfung Ihrer Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), mit denen Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder beides) gespeichert, verarbeitet oder übertragen werden.

Version 2025/01

Swisscard AECS GmbH • Postfach 227 • CH-8810 Horgen • swisscard.ch
American Express Cards, issued by Swisscard AECS GmbH

2500M/09.2025