DIRECTIVE DE SWISSCARD CONCERNANT LE RESPECT DES PRESCRIPTIONS DE SÉCURITÉ PCI DSS POUR LES PARTENAIRES CONTRACTUELS

Généralités
Swisscard AECS Sàrl (Swisscard) s'engage depuis de nombreuses années à protéger les données des titulaires de carte pour assurer une sécurité maximale. L'utilisation non autorisée de données a un impact négatif sur les titulaires de cartes, les partenaires contractuels, les prestataires de services et les émetteurs de cartes. Les Payment Card Industry Data Security Standards (PCI DSS), introduits pour faire face à ce risque, contribuent à renforcer la confiance des clients, à accroître la rentabilité et à renforcer la réputation d'une entreprise. Chez Swisscard, nous savons que nos partenaires contractuels partagent ces préoccupations. Par conséquent, dans le cadre de la responsabilité qui vous incombe, nous vous demandons de respecter les dispositions relatives à la protection des données prévues dans les Conditions générales d'acceptation des cartes American Express et dans la présente directive que nous réviserons en tant que de besoin.

PCI DSS
Les Payment Card Industry Data Security Standards (PCI DSS) ont été élaborés il y a plusieurs années par Visa International, MasterCard, American Express, JCB et Discover afin de favoriser l'introduction à l'échelle mondiale de mesures uniformes de sécurité des données et de protéger les données de cartes de manière préventive, améliorant ainsi la sécurité lors du traitement des données de cartes. Ils sont publiés par le Payment Card Industry Security Standards Council et règlent les exigences techniques et opérationnelles applicables à toutes les parties qui conservent, traitent et transmettent des données de cartes.
La version la plus récente des exigences détaillées peut être consultée à tout moment sous www.pcisecuritystandards.org.

Responsabilités
Les PCI DSS sont obligatoires pour tous nos partenaires contractuels, banques, sous-traitant des données et fournisseurs de services de paiement qui conservent, traitent ou transmettent des données de titulaires de cartes à leurs propres fins ou pour le compte d'autres organisations. Il appartient au partenaire contractuel de se conformer aux PCI DSS. Les partenaires contractuels seront également responsables du respect des PCI DSS par les tiers qu'ils mandatent, p. ex. les fournisseurs de services de paiement, qui traitent, conservent ou transmettent des données de cartes pour leur compte. Les coûts des mesures de certification sont entièrement supportés par le partenaire contractuel ou le tiers mandaté.

Comment procéder?
Pour démontrer sa conformité aux PCI DSS, le partenaire contractuel est tenu de documenter les mesures de sécurité qu'il a prises (mesures de certification). Le tableau ci-dessous montre aux partenaires contractuels les obligations qui leur incombent et les documents qu'ils doivent présenter pour démontrer leur conformité aux PCI DSS, en fonction de leur volume de transactions annuel.
Il est important de noter que les partenaires contractuels de niveau 3 et 4 n'ont à fournir des documents de certification que sur demande de Swisscard, mais demeurent néanmoins responsables et soumis à toutes les autres dispositions des PCI DSS. Swisscard informera ces partenaires contractuels par écrit au moins nonante (90) jours avant la remise requise de tels documents.

Niveau/Transactions American Express annuelles	Rapport sur l'évaluation sur place de la conformité (Report on Compliance, ROC)	Questionnaire d'auto-évaluation (Self Assessment Questionnaire, SAQ) ET contrôle trimestriel	Attestation STEP pour les commerçants admissibles
Niveau 1 **2.5 millions ou plus**	Obligatoire	Non applicable	Facultatif (remplace le ROC)
Niveau 2 **50 000 à 2.5 millions**	Facultatif	SAQ obligatoire (sauf en cas de présentation d'une évaluation sur place): contrôle obligatoire avec certains types de SAQ.	Facultatif (remplace le SAQ et le contrôle de réseau ou le ROC)
Niveau 3 **10 000 bis 50 000**	Facultatif	SAQ facultatif (obligatoire si Swisscard ou American Express le demande): contrôle obligatoire avec certains types de SAQ.	Facultatif (remplace le SAQ et le contrôle de réseau ou le ROC)
Niveau 4 **10 000 ou moins**	Facultatif	SAQ facultatif (obligatoire si Swisscard ou American Express le demande): contrôle obligatoire avec certains types de SAQ.	Facultatif (remplace le SAQ et le contrôle de réseau ou le ROC)

Que faire en cas de violation des données?
Vous devez informer Swisscard **sans délai, mais au plus tard dans les vingt-quatre (24) heures suivant** la découverte de la violation de données, par téléphone au **044 659 64 44** (service téléphonique 24 heures/24).

Pour les questions et les informations complémentaires
Pour toute question relative aux PCI, veuillez contacter notre centre de service au **044 659 64 44** (service téléphonique 24 heures/24)
Pour de plus amples informations, veuillez consulter la Politique de sécurité des données d'American Express (Data Security Operating Policy, DSOP) disponible en ligne à l'adresse www.americanexpress.com. Veuillez noter que la documentation ne doit pas être remise directement à American Express mais à Swisscard. Veuillez nous contacter pour de plus amples informations.

Glossaire
Evaluation annuelle de sécurité sur place: L'évaluation annuelle de sécurité sur place consiste en un contrôle approfondi de sécurité dans vos locaux de vos appareils, systèmes et réseaux (et composants associés) utilisés pour conserver, traiter ou transférer des données de titulaires de cartes ou des données d'authentification confidentielles (ou les deux).

Questionnaire annuel d'auto-évaluation: Le questionnaire d'auto-évaluation PCI DSS (SAQ) est utilisé pour contrôler vous-même vos appareils, systèmes et réseaux (et composants associés) utilisés pour conserver, traiter ou transférer des données de titulaires de cartes ou des données d'authentification confidentielles (ou les deux).

Version 2025/01

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

2500M/09.2025