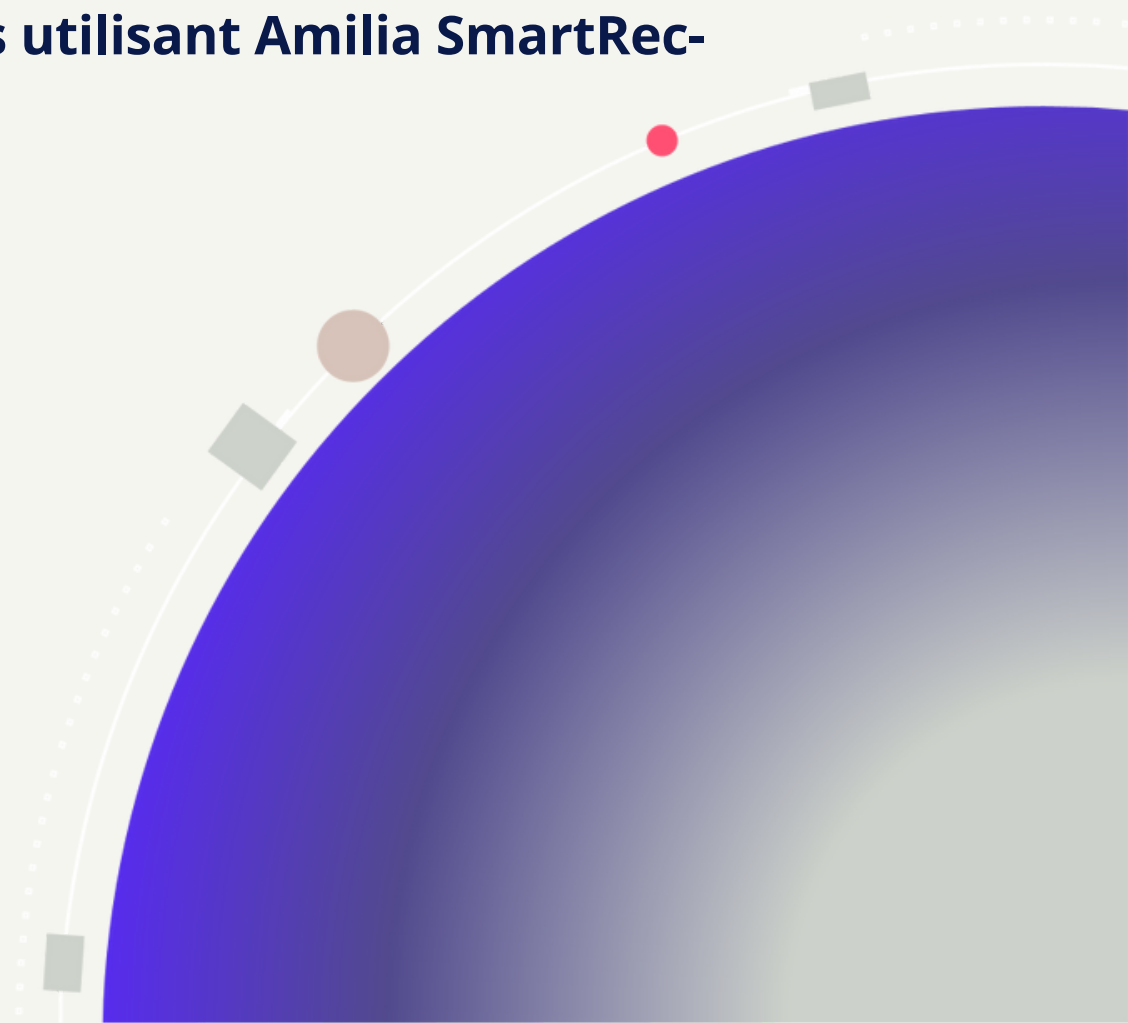


Lorsque vous acceptez les paiements par carte dans la boutique Amilia SmartRec (uniquement)

-Ce guide est adapté aux commerçants utilisant Amilia SmartRec-

Type QAE A (SAQ A) - Guide de réponses
PCI v4.0

January 2024 – PCI v3.2.1



QAÉ A - Guide de réponses

Une fois votre compte marchand connecté, vous recevrez les informations de connexion à votre compte PCI par courriel.

- Vous y trouverez votre nom d'utilisateur et votre numéro de marchand.
- Cliquez sur le lien dans le courriel pour créer un mot de passe. Assurez-vous de suivre les instructions à l'écran.
- Lors de votre première connexion, vérifiez vos coordonnées pour vous assurer qu'elles sont exactes.

QAÉ A - Guide de réponses

- Cliquez sur « **Gérer** » pour commencer.
Le profil dresse un tableau de comment votre entreprise gère les paiements par carte.
- Suivez ce guide (SAQ type A/QAÉ A) si votre entreprise accepte les paiements par carte **uniquement** à partir de votre boutique en ligne Amilia SmartRec.



Le profil de votre entreprise

Plus d'informations Gérer

←

Et ensuite ?

- 1 Nous vous poserons quelques questions
La plupart d'entre elles concernent le traitement des paiements par carte de crédit et de débit dans votre entreprise. Vos réponses nous permettent de cerner le niveau de risque pour la sécurité de votre entreprise, c'est pourquoi nos questions se limitent aux sujets qui lui sont pertinents.
- 2 Laissez-nous vous aider à protéger votre entreprise
Afin de vous aider à comprendre quels sont les secteurs potentiellement à risque dans votre entreprise, vous serez soumis à une évaluation de la sécurité et à des analyses de votre système, au besoin.
- 3 Confirmation de la sécurité de l'entreprise
Nous vous demanderons de confirmer vos réponses et de valider toutes les tâches d'analyse demandées. La norme PCI DSS regroupe ces éléments sous la mention Attestation de conformité (AOC).

Démarrer le questionnaire de profil

QAÉ A - Guide de réponses

PRIÈRE DE LIRE : Mise à jour PCI DSS 4.0

Nous avons mis à jour notre processus de profilage pour nous conformer aux exigences de la version 4.0 de la Norme de Sécurité des Données de l'Industrie des Cartes de Paiement (PCI DSS).

Si vous avez déjà suivi cette procédure, veuillez reconfirmer vos réponses. Il se peut que vous deviez répondre à des questions supplémentaires afin de déterminer correctement votre niveau de conformité à la dernière version de la norme.

Veuillez vous référer au Conseil des Normes de Sécurité PCI [PCI DSS v4.0 Resource Hub](#) pour plus d'informations.

Nous avons également mis à disposition des ressources supplémentaires [ici](#).



Je comprends

Suivant

- La norme PCI est désormais passée de la v3.2.1 à la v.4.0. Le portail PCI a été mis à jour par rapport aux dernières normes de conformité.
- Veuillez lire le message ci-dessus et cliquer sur « **Je comprends** » pour continuer.

QAÉ A - Guide de réponses

Choisissez une méthode d'évaluation

☒ **Guidez-moi** - Sélectionnez cette option pour utiliser notre outil de profilage afin de vous aider à déterminer l'étendue de votre évaluation PCI DSS.

☐ **Expert** - Sélectionnez cette option si vous connaissez déjà le type de SAQ applicable à votre entreprise, sans être guidé par notre outil de profilage. Vous devrez répondre à toutes les exigences du questionnaire d'évaluation.

☐ **Télécharger** - Sélectionnez cette option pour télécharger votre questionnaire d'auto-évaluation (SAQ) ou votre attestation de conformité (AoC) PCI DSS en cours de validité et provenant d'un programme externe.

[Précédent](#) [Suivant](#)

- « **Guidez-moi** » - pour finaliser votre conformité à l'aide du portail PCI. (Recommandé)
- « **Expert** » - si vous ne souhaitez pas utiliser l'outil de profilage pour pré-remplir certaines de vos exigences PCI. (non recommandé)
- « **Télécharger** » - si vous avez déjà terminé votre conformité pour l'année à venir et souhaitez télécharger la documentation requise.

QAÉ A - Guide de réponses

Les instructions qui suivent correspondent à l'option « Guidez-moi »

Méthodes de perception de cartes bancaires ?

Veuillez sélectionner tous les moyens par lesquels vous utilisez les cartes de paiement dans votre entreprise aujourd'hui. Veuillez noter qu'il s'agit uniquement des cartes de marque (Visa et MasterCard, par exemple) et non des autres types de paiement (PayPal et Google Wallet, par exemple, ne s'appliquent pas).

☐



Face à face (le client est présent et la carte de paiement est insérée, appliquée ou balayée pour effectuer la transaction. Cela inclut les kiosques non surveillés.) ?

☒



Paielements en ligne (y compris site web/boutique de commerce électronique, application mobile pour les consommateurs, etc.) ?

☐



Paielements de commandes par carte par courriel et/ou par téléphone ?

Précédent

Suivant

Puisque vous n'acceptez les paiements par carte que dans la boutique en ligne Amilia SmartRec (via l'API de Paysafe), **veuillez sélectionner la 2e option - Paiements en ligne.**

QAÉ A - Guide de réponses

Pay by Link (Paiement par Lien)

Vos clients peuvent-ils effectuer des paiements par carte via une solution Pay by Link (un lien de paiement sécurisé est envoyé au client pour lui permettre d'effectuer un paiement) ? ?

☐ Oui ☒ Non

PrécédentSuivant

Cette question vous demande si vous fournissez à vos clients un lien de paiement sécurisé pour traiter leur paiement. Puisque vous n'acceptez les paiements par carte que dans la boutique en ligne Amilia SmartRec (via l'API de Paysafe), **veuillez répondre à cette question par « Non ».**

QAÉ A - Guide de réponses

Organisation de commerce électronique ?

Veillez sélectionner tous les moyens par lesquels les clients effectuent des paiements par carte en ligne à votre entreprise.

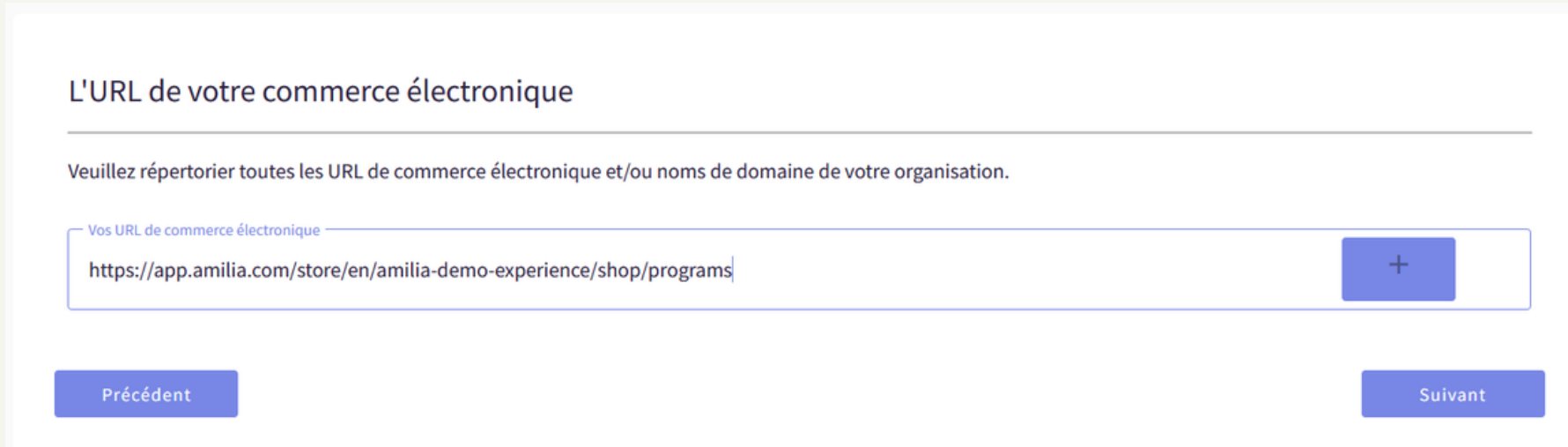
☒ Mes clients effectuent des paiements en ligne à mon entreprise via un site web accessible à l'aide d'un navigateur web.

☐ Mes clients effectuent des paiements en ligne à mon entreprise via une application mobile téléchargée sur leur propre appareil à partir d'un App Store.

Précédent Suivant

- Puisque vous utilisez uniquement la boutique en ligne Amilia SmartRec (via l'API de Paysafe) pour accepter les paiements par carte, **veuillez sélectionner la première option.**

QAÉ A - Guide de réponses



The screenshot shows a web form titled "L'URL de votre commerce électronique". Below the title is a horizontal line. Underneath the line is the instruction: "Veuillez répertorier toutes les URL de commerce électronique et/ou noms de domaine de votre organisation." Below this instruction is a text input field with the placeholder "Vos URL de commerce électronique". The field contains the URL "https://app.amilia.com/store/en/amilia-demo-experience/shop/programs". To the right of the input field is a blue button with a white "+" sign. Below the input field and the "+" button are two blue buttons: "Précédent" on the left and "Suivant" on the right.

- Veuillez saisir l'URL de votre boutique en ligne Amilia SmartRec. Vous pouvez ajouter plusieurs URL si vous possédez plusieurs boutiques en ligne Amilia SmartRec.
- Sélectionnez ensuite l'icône «+» pour l'ajouter. Sélectionnez « Suivant » lorsque vous êtes prêt à continuer.

QAÉ A - Guide de réponses

Gestion d'un site de commerce électronique

Votre site de paiement en ligne est-il entièrement géré, exploité et entretenu par un tiers ? Cela signifie que vous avez complètement externalisé toutes les opérations liées à votre site de paiement en ligne. 

☒ Oui ☐ Non

[Précédent](#) [Suivant](#)

- Puisque vous utilisez votre boutique en ligne Amilia SmartRec (via l'API de Paysafe) pour accepter les paiements par carte, **veuillez répondre « Oui » à cette question.**

QAÉ A - Guide de réponses

Votre fournisseur de services de commerce électronique externalisé ?

Votre fournisseur de services de commerce électronique externalisé est-il conforme à la norme PCI DSS pour les services qu'il vous fournit ?

☒ Oui ☐ Non

Précédent Suivant

- En tant que fournisseur de services de commerce électronique, Amilia SmartRec est conforme au niveau 1 PCI. Veuillez visiter trust.amilia.com pour obtenir une copie de notre attestation de conformité dans la section « Ressources ».
- **Veuillez répondre « Oui » à cette question.**

QAÉ A - Guide de réponses

L'analyse ASV est-elle effectuée par le prestataire de votre site de commerce électronique ? 

Pouvez-vous vérifier ou fournir la preuve que votre prestataire de solutions de commerce électronique effectue une analyse de vulnérabilité sur votre site web au moins une fois par trimestre, conformément aux directives du programme ASV, dans le but de maintenir la conformité à la norme PCI DSS ?

☒ Oui ☐ Non

[Précédent](#) [Suivant](#)

- En tant que fournisseur de services de commerce électronique, Amilia SmartRec est conforme au niveau 1 PCI et effectue des analyses externes trimestrielles de votre boutique en ligne.
- Amilia SmartRec.
- **Veillez répondre « Oui » à cette question.**

QAÉ A - Guide de réponses

- Pour sélectionner votre fournisseur, taper « **Paysafe** » dans le champ.
- Veuillez choisir la 2e option - **Paysafe Paysafe Group (prev.Netbanx)**

Fournisseur de services de paiement ?

Veuillez indiquer le nom de votre fournisseur de services de paiement :

Paysafe|

Paysafe Paysafe Group (prev. Netbanx) ✕

☐ Paysafe Group Plc.

☒ Paysafe Paysafe Group (prev. Netbanx)

☐ PAYSAFE SERVICES (US) CORP.

Précédent Suivant

QAÉ A - Guide de réponses

Votre portail/processeur de paiement est-il conforme à la norme PCI DSS ? 

Pouvez-vous vérifier si, ou détenez-vous une preuve qui pourrait vous laisser croire que, votre fournisseur de services de paiement est conforme à la norme PCI DSS en ce qui concerne les services qu'il vous offre?

☒ Oui ☐ Non

[Précédent](#) [Suivant](#)

- Paysafe est un fournisseur de services de paiement de niveau 1 – **veuillez répondre « Oui » à cette question.** Vous pouvez obtenir une copie de l’attestation de conformité de Paysafe auprès de notre centre de confiance sur trust.amilia.com dans la section « Ressources ».

QAÉ A - Guide de réponses

- Vous ne devez **en aucun cas** envoyer, recevoir, transmettre ou stocker les données du titulaire de la carte par voie électronique. Cela expose les données de votre organisation et de vos clients au risque d'être priatées par des individus malveillants.

Autres utilisations des numéros de carte ?

Permettez-vous que quiconque de votre entreprise transmette ou reçoive des numéros complets de carte par courriel ou messagerie instantanée?

☐ Oui ☒ Non

Est-ce que votre entreprise transmet ou reçoit des données de titulaires de carte par voies électroniques? De quelle autre façon reçoivent-ils des données; sur CD-ROM, lecteur USB, courriel, réseau interne ou Internet? ?

☐ Oui ☒ Non

PrécédentSuivant

- Répondez « Non » aux deux questions.

QAÉ A - Guide de réponses

- Si vous n'avez pas de politique de sécurité des informations, vous pouvez télécharger le modèle de politique fourni.
- Votre organisation doit disposer d'une politique de sécurité des informations qui est lue, signée et datée par tous les employés qui gèrent les paiements par carte.

Politique de sécurité des renseignements

La norme Payment Card Industry Data Security Standard (PCI DSS) vous oblige à vous doter d'une politique de sécurité des renseignements qui couvre tous les aspects pertinents de la norme. Nous pouvons vous proposer un modèle de politique si vous n'en avez pas déjà un. ?

☒ Je ne dispose actuellement pas d'une politique en matière de sécurité; je me servirai du modèle pour en mettre une en œuvre. [Téléchargement](#) ←

☐ Je dispose déjà d'une politique en matière de sécurité de l'information qui couvre TOUTES les dispositions pertinentes de la norme PCI DSS

☐ Je n'ai pas actuellement une politique de sécurité de l'information en place qui couvre toutes les clauses pertinentes de la Payment Card Industry Data Security Standard (PCI DSS), mais je ne veux pas utiliser celui fourni comme base de ma politique.

Précédent Suivant

QAÉ A - Guide de réponses

Politique en matière de mot de passe

Appliquez-vous un mot de passe d'une longueur minimale de sept caractères, contenant à la fois des caractères numériques et alphabétiques, pour les comptes d'utilisateurs sur tous les terminaux de paiement, les ordinateurs et les systèmes de votre entreprise ? 

☒ Oui ☐ Non

Veuillez noter : Il s'agit de la meilleure pratique jusqu'au 31 mars 2025, date à partir de laquelle la complexité du mot de passe exigera une longueur minimale de douze caractères (lorsque douze caractères sont pris en charge, sinon un minimum de huit caractères est requis).

Précédent

Suivant

- À partir du 31 mars 2025, vous devrez mettre à jour les exigences en matière de mots de passe au sein de votre entreprise pour garantir qu'elle est protégée contre les individus malveillants.
- Toute personne disposant d'un accès administrateur à votre site Web devra disposer d'un mot de passe d'une longueur de 12 caractères, au lieu de 8.
- Comme il s'agit d'une exigence future, cette question n'affectera pas votre statut de conformité.
- **Veuillez répondre à cette question telle qu'elle s'applique à votre entreprise aujourd'hui.**

QAÉ A - Guide de réponses

C'est la dernière question du profil d'entreprise.

Comme votre organisation n'accepte les paiements par carte que dans la boutique Amilia SmartRec, **ces réponses suffisent pour les trois champs :**

‘Configuration du commerce électronique, système Paysafe dot JS acceptant les paiements par carte, iFrame en place, les systèmes sont mis à jour tout au long de l'année, aucune donnée de titulaire de carte n'est stockée, il y a X NOMBRE d'employés qui ont accès dans l'arrière boutique.’

Un résumé de votre méthode de gestion des paiements par carte et des endroits concernés

Veillez fournir les renseignements requis ci-dessous. Ils feront partie de votre attestation de conformité.

Veillez énumérer les types de locaux de votre entreprise ainsi que les principaux emplacements qui sont concernés par l'évaluation de conformité à la norme PCI DSS (p. ex., points de vente au détail, bureaux administratifs, centres de données, centres d'appels, etc.) ?

Configuration du commerce électronique, système Paysafe dot JS acceptant les paiements par carte, iFrame en place, les systèmes sont mis à jour tout au long de l'année, aucune donnée de titulaire de carte n'est stockée, il y a X NOMBRE d'employés qui ont accès dans l'arrière boutique.

285/4000

Comment, et à quel titre, votre entreprise entrepose, traite et transmet-elle les données des titulaires de carte? ?

Configuration du commerce électronique, système Paysafe dot JS acceptant les paiements par carte, iFrame en place, les systèmes sont mis à jour tout au long de l'année, aucune donnée de titulaire de carte n'est stockée, il y a X NOMBRE d'employés qui ont accès dans l'arrière boutique.

285/4000

Fournissez une description détaillée de l'environnement d'affaires de votre entreprise qui s'applique à l'évaluation de conformité à la norme PCI DSS. Décrivez par exemple le type d'équipement utilisé pour le traitement, l'entreposage et la transmission de données de titulaires de carte, comme les dispositifs PDV, les bases de données et les serveurs Web. Expliquez le processus de connexion externe et interne.

Configuration du commerce électronique, système Paysafe dot JS acceptant les paiements par carte, iFrame en place, les systèmes sont mis à jour tout au long de l'année, aucune donnée de titulaire de carte n'est stockée, il y a X NOMBRE d'employés qui ont accès dans l'arrière boutique.

285/4000

QAÉ A - Guide de réponses



- Une fois que toutes les étapes ont été complétées dans le profil d'entreprise, vous verrez qu'il reste quelques questions à répondre dans l'**évaluation de sécurité**.
- Cliquez sur « **Gérer** » pour commencer l'évaluation de sécurité.

QAÉ A - Guide de réponses

Montrez-moi :
Questions sans réponse seulement

Afficher le texte d'aide :

Veuillez noter que certaines questions auxquelles une réponse a été donnée peuvent être affichées pour des fins de contexte

Protéger les Données de Compte
Exigence 3 : Protéger les Données de Compte Stockées

Les processus et mécanismes de protection des données de compte stockées sont définis et compris

Le stockage des données de compte est réduit au minimum.

Groupe de question 3.2.1

 Aide pour répondre à cette exigence

Sections

- ✓ Créer et Maintenir un Réseau et des Systèmes Sécurisés
- 1 Protéger les Données de Compte
- ✓ Maintenir un Programme de Gestion des Vulnérabilités
- 2 Mettre en Œuvre des Mesures Robustes de Contrôle d'Accès
- ✓ Maintenir une Politique de Sécurité des Informations
- ✗ Attester de votre conformité

- Dans la zone « Sections » ci-dessus, vous aurez quelques questions liées à « protéger les données de compte » et à « mettre en œuvre des mesures robustes de contrôle d'accès ».

QAÉ A - Guide de réponses

Cette question vous demande si vous avez mis en place une politique de conservation des données qui couvre tous les installations de votre entreprise susceptibles de stocker des informations sensibles.

- **Veillez répondre « N/A » à cette question et écrire « Mon organisation utilise uniquement la boutique en ligne Amilia SmartRec pour gérer les paiements par carte. Amilia ne stocke ni ne transmet les données de compte ».**

3.2.1

Le stockage des données de compte est réduit au minimum grâce à la mise en œuvre de politiques, procédures et processus de conservation et d'élimination des données qui incluent au moins les éléments suivants :

- Couverture de tous les emplacements des données de compte stockées.
- Couverture de toutes les données d'authentification sensibles (SAD) stockées avant la fin de l'autorisation. Cette note est une bonne pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes d'Applicabilité ci-dessous pour plus de détails.
- Limiter la quantité de stockage des données et la durée de conservation à ce qui est requis pour les exigences légales ou réglementaires et/ou commerciales.
- Des exigences de rétention spécifiques pour les données de compte stockées qui définissent la durée de la période de conservation et incluent une justification commerciale documentée.
- Des processus de suppression sécurisée ou rendre des données de compte irrécupérables lorsqu'elles ne sont plus nécessaires conformément à la politique de conservation. Un processus pour vérifier, au moins une fois tous les trois mois, que les données de compte stockées dépassant la période de conservation définie ont été supprimées en toute sécurité ou rendues irrécupérables.

J'ai mis un contrôle de compensation en œuvre

N.A.

Non

Oui

QAÉ A - Guide de réponses

- Si vous avez répondu « Non » à l'application d'une politique de mot de passe dans votre profil d'entreprise, vous verrez cette question dans votre évaluation de sécurité.
- **Veillez répondre « Oui » à cette question ou « N/A ».** Si vous répondez « Non », vous échouerez à l'évaluation de sécurité.

8.3.6

Si des mots de passe/phrases secrètes sont utilisés comme facteurs d'authentification pour répondre à l'exigence 8.3.1, ils devront répondre au niveau de complexité minimum suivant :

- Une longueur minimale de 12 caractères (ou SI le système ne prend pas en charge 12 caractères, une longueur minimale de huit caractères).
- Contenir à la fois des caractères numériques et alphabétiques.

J'ai mis un contrôle de compensation en œuvre

N.A.

Non

Oui

QAÉ A - Guide de réponses

- **Veillez répondre « N/A » à cette question et écrire « Mon organisation utilise uniquement la boutique en ligne Amilia SmartRec pour gérer les paiements par carte, qui ne stocke ni ne transmet les données des titulaires de cartes ».**

9.4.1.1

Les sauvegardes sur des supports hors ligne avec les données des titulaires de cartes sont stockées dans un emplacement sécurisé.

J'ai mis un contrôle de compensation en œuvre

N.A.

Non

Oui

QAÉ A - Guide de réponses

Montrez-moi :
Questions sans réponse seulement

Afficher le texte d'aide :

Veuillez noter que certaines questions auxquelles une réponse a été donnée peuvent être affichées pour des fins de contexte

Mettre en Œuvre des Mesures Robustes de Contrôle d'Accès

i Aucune question de cette section n'a été laissée sans réponse

Attention ! Il reste des questions répondues par « Non », ce qui signifie que votre évaluation de sécurité ne sera pas complète tant que les tâches de remédiation relatives aux questions répondues par « Non » ne seront pas exécutées

Sections

- ☒ Créer et Maintenir un Réseau et des Systèmes Sécurisés
- ☒ Protéger les Données de Compte
- ☒ Maintenir un Programme de Gestion des Vulnérabilités
- ☒ Mettre en Œuvre des Mesures Robustes de Contrôle d'Accès
- ☒ Maintenir une Politique de Sécurité des Informations
- ☒ **Attester de votre conformité**

- Une fois que toutes les questions auront été répondues dans cette section, vous pourrez alors confirmer votre conformité et compléter un dernier élément pour être validé pour l'année à venir.
- **Veuillez cliquer sur la section « Attester de votre conformité » comme indiqué ci-dessus.**

QAÉ A - Guide de réponses

Attester votre conformité

Veillez remplir les sections incomplètes du formulaire ci-dessous

✓ Renseignements détaillés sur votre organisation

Nom de la société	Nom du contact*
123Test	Test Amilia
Poste	Numéros de téléphone
	1888-851-7558
Adresse courriel	Adresse professionnelle
	128 Vision Park Blvd
Suite 300	Conroe
Texas	77384
Pays	
États-Unis	

- Examinez attentivement les coordonnées, car elles seront ajoutées à la signature électronique de votre attestation de conformité.
- **Veillez vous assurer de remplir tous les détails.**

QAÉ A - Guide de réponses

- Une fois que vous avez mis à jour les informations de contact, faites défiler vers le bas et cliquez sur le bouton « **Attester** »

The screenshot displays a web form for the QAÉ A submission. It features five expandable sections, each with a checkmark icon and a downward arrow. The sections are: 'Type d'entreprise du commerçant', 'Description de l'environnement', 'Admissibilité à répondre au QAÉ A', 'Reconnaissance de l'état et attestation du commerçant', and 'Nom du Représentant Exécutif du Commerçant'. The fifth section, 'Attestation du commerçant', is expanded, revealing a green confirmation box. This box contains a green checkmark icon, the heading 'Renseignements pour la soumission.', and two paragraphs of text. The first paragraph states that, based on the QAÉ A results from April 9, 2024, the signatories identified in section 1.1 confirm the state of conformity for the identified entity. The second paragraph states that all sections of the QAÉ A of the PCI DSS are completed, all questions have been answered affirmatively, and the entity is required to maintain conformity with the PCI DSS standard at all times. A blue 'Attester' button is located at the bottom right of the form.

✓ Type d'entreprise du commerçant

✓ Description de l'environnement

✓ Admissibilité à répondre au QAÉ A

✓ Reconnaissance de l'état et attestation du commerçant

✓ Nom du Représentant Exécutif du Commerçant

✗ Attestation du commerçant

✓ Renseignements pour la soumission.

Compte tenu des résultats du QAÉ A en date du Apr 9, 2024, les signataires identifiés dans la partie 1.1, le cas échéant, confirment l'état de conformité suivant pour l'entité identifiée dans la partie 2 du présent document en date du Apr 9, 2024 :

Conforme : toutes les sections du QAÉ du PCI DSS sont remplies, toutes les questions ont été répondues par l'affirmative. Vous êtes tenu de maintenir la conformité avec la norme PCI DSS à tout moment.

Attester

QAÉ A - Guide de réponses

Une fois toutes les étapes terminées, vous serez redirigé vers cet écran qui indique que votre organisation est désormais conforme pour l'année à venir.

Lorsqu'une action sera requise dans le portail PCI, vous recevrez un courriel pour vous informer.

PaysafeMID: 123Test



Vous êtes conforme

Valable jusqu'au
9 Avril 2025

[TÉLÉCHARGEZ AOC](#)

VOUS ÊTES MAINTENANT CONFORME

Vous pouvez relaxer, vous avez terminé! Bon travail.



Voici les outils de conformité à votre disposition



Le profil de votre entreprise

Terminé
Type de QAÉ A

[Plus d'infos](#) [Gérer](#)



Remplir l'évaluation de sécurité

Dernière attestée
Apr 9, 2024, 8:29:43 PM

[Plus d'infos](#) [Gérer](#)