Bookassist®

Politique Extranet Bookassist

Dernière mise à jour : 25 Mai 2018

Cette politique inclut :

1) Les Termes & conditions pour l'utilisation du Système d'Administration Bookassist (« Système »)

2) Les informations sur la protection des données pour les employés / le personnel autorisé accédant au système et / ou au Système de Gestion de Contenu Bookassist (« CMS »)

3) Les notes explicatives sur la politique du mot de passe pour l'utilisation du Système

Notez qu'en utilisant le Système d'Administration Bookassist (« Système »), vous reconnaissez accepter les Termes & conditions décrits ici.

Le Système donne accès aux données personnelles en fonction des obligations contractuelles définies dans le contrat Bookassist avec le fournisseur d'Hébergement Hôtelier et conformément aux conditions de traitement et de sécurité des données Bookassist (https://bookassist.org/dp).

Conditions d'utilisation du Système d'Administration Bookassist (« Système »)

1. **Exigences PCI DSS (normes de sécurité des données de l'industrie des cartes de paiement)**

   a) Bien que Bookassist s'efforce de respecter pleinement les conditions fixées par les normes de sécurité des données de l'industrie des cartes de paiement (PCI DSS) pour le traitement des paiements en ligne, le fournisseur Hôtelier est entièrement responsable de l'utilisation correcte des données personnelles fournies dans le Système, conformément à la législation pertinente sur la protection des données.

   b) Le fournisseur Hôtelier doit nommer un administrateur pour le système qui sera responsable de contrôler l'accès des autres employés et / ou du personnel autorisé au Système (les « Utilisateurs »).

   c) Le fournisseur Hôtelier est entièrement responsable du bon fonctionnement des exigences PCI DSS mises en œuvre par Bookassist en ce qui concerne l'administration des Utilisateurs ayant accès au Système, la protection des noms d'utilisateur et mots de passe du système, et en particulier, le contrôle des utilisateurs ayant accès aux détails de la carte de crédit du titulaire. Notamment, le fournisseur Hôtelier garantit qu'il :

      - respectera les exigences de sécurité PCI DSS
      - reconnaît qu'il est responsable de la sécurisation des données du titulaire de la carte
      - reconnaît que les données du titulaire de la carte ne doivent être utilisées que pour faciliter la réalisation d'une transaction, soutenir un programme de fidélité, répondre à un service de contrôle des fraudes ou pour des usages spécifiquement requis par la loi
      - fournira une coopération et un accès complets pour effectuer un examen approfondi de la sécurité après une intrusion dans la sécurité, auprès d'un représentant de

l'industrie des cartes de paiement ou d'un tiers approuvé par l'industrie des cartes de paiement

- reconnaît que ces obligations de protéger la confidentialité des données du titulaire de la carte survivront à la résiliation de tout autre accord contractuel avec Bookassist.

d) Toute violation des normes, procédures ou lignes directrices établies en vertu de la présente politique doit être présentée à la direction du fournisseur Hôtelier pour prendre les mesures appropriées. Cela pourrait entraîner des mesures disciplinaires, y compris le renvoi ou l'interruption du service et / ou des poursuites judiciaires.

2. Accès selon le besoin de savoir

L'accès au système à un niveau particulier ne devrait être accordé qu'aux Utilisateurs qui ont spécifiquement besoin d'accéder à ce niveau pour effectuer leur travail.

3. Accès et restrictions aux données

a. L'accès ne devrait être accordé que si le fournisseur Hôtelier l'autorise.

b. Les données de la carte de crédit du client ne peuvent être consultées que dans la limite d'un mois après la date de départ de la réservation. Après cela, les données sont automatiquement supprimées du système Bookassist et ne peuvent pas être récupérées.

c. Toutes les autres données personnelles du client sont anonymisées 12 mois après la date de départ.

4. Connexions individuelles

Les connexions doivent être uniques pour chaque utilisateur. Les utilisateurs ne peuvent pas partager leur connexion avec quelqu'un d'autre.

5. Utilisateurs inactifs

Les connexions doivent être immédiatement supprimées pour les utilisateurs qui n'en ont plus l'usage ou qui ont quitté l'hôtel.

6. Nouveaux utilisateurs

Lorsque les connexions sont configurées pour le Système, l'utilisateur est obligé de lire, comprendre et accepter les conditions énumérées ci-dessus.

Informations sur la protection des données pour les employés / le personnel autorisé accédant au Système et / ou au Système de Gestion de Contenu (« CMS »)

1. Informations collectées sur les employés / le personnel autorisé (« Utilisateurs ») accédant au Système ou au CMS et Pourquoi elles sont recueillies et traitées

a) Les utilisateurs qui accèdent au Système ou au CMS doivent fournir leur nom, leur adresse électronique et leur numéro de téléphone. En outre, le Système et le CMS enregistrent les informations du journal de tous les accès et activités.

b) Cette collecte et ce traitement de données sont nécessaires pour la fonctionnalité du Système et du CMS et pour analyser les problèmes afin de les solutionner.

2. Comment les données de l'Utilisateur peuvent être utilisées et Qui a accès

Les données de l'utilisateur doivent être utilisées pour soutenir le fonctionnement du Système et du CMS. Le fournisseur Hôtelier peut demander l'accès aux données de l'Utilisateur. Veuillez contacter le fournisseur Hôtelier concerné pour plus de détails sur l'utilisation de ces données. Veuillez noter que si le fournisseur Hôtelier a demandé les données de l'Utilisateur, le fournisseur Hôtelier peut conserver l'accès à celles-ci pour une période de conservation différente.

3. Droits de l'utilisateur

Les Utilisateurs ont le droit de demander l'accès, la rectification et l'effacement de leurs données, ainsi que le droit à la portabilité des données, et le droit de déposer une plainte auprès de l'autorité de surveillance compétente conformément aux exigences pertinentes en matière de protection des données.

4. Rétention

Toutes les données énumérées à la section 1 doivent être conservées par Bookassist pendant deux ans après la date d'expiration de l'utilisateur.

5. Contact

Vous pouvez envoyer un e-mail au contact de la protection des données Bookassist à l'adresse dpo@bookassist.com si vous avez besoin de plus d'informations ou si vous souhaitez exercer vos droits.

Notes explicatives sur la politique du mot de passe pour l'utilisation du Système

Les normes PCI signifient que les mots de passe que vous utilisez dans le Système doivent répondre à un ensemble de règles particulières. La procédure de connexion sur le Système garantit que les normes PCI sont respectées. La vérification de connexion de Bookassist validera le nom de l'Utilisateur et le mot de passe, et, pour les erreurs, des messages clairs s'afficheront à l'écran expliquant celles-ci et comment les corriger.

1. Mots de passe forts

Sélectionnez des mots de passe forts avec ces caractéristiques :

- utiliser des caractères majuscules et minuscules, ainsi que des chiffres ou des signes de ponctuation
- n'utilisez pas d'informations personnelles ou de mots d'usage courant ou trouvés dans un dictionnaire
- ne partagez pas de mot de passe avec qui que ce soit
- n'écrivez pas un mot de passe ou ne le stockez pas en ligne.

2. Âge du mot de passe

Tous les 90 jours, le système vous demande de changer votre mot de passe. Des instructions claires vous guideront tout au long de ce processus.

3. Format du mot de passe

La longueur du mot de passe doit comporter au moins 7 caractères, avec un minimum de 1 chiffre et 1 caractère alphabétique. Si vous changez votre mot de passe et qu'il ne répond pas à ces exigences, un message s'affiche à l'écran, vous indiquant ce qu'il faut faire pour que le mot de passe soit valide.

4. Historique du mot de passe

Lorsque vous modifiez votre mot de passe, le système vérifie qu'il ne correspond à aucun de vos 4 derniers mots de passe.

5. Tentatives de connexion

Si vous vous connectez et que vous saisissez le mauvais mot de passe, vous avez un total de 6 tentatives avant d'être bloqué. Si cela se produit, demandez à votre Administrateur de réinitialiser le mot de passe et attendez 30 minutes pour vous reconnecter.

6. Heure de verrouillage

Si votre accès au Système a été verrouillé parce que vous avez saisi le mauvais mot de passe à 6 reprises, vous devez attendre 30 minutes avant de pouvoir vous reconnecter, même après que l'Administrateur ait réinitialisé votre mot de passe.

7. Délai d'expiration de la session

PCI nous oblige à limiter une session de connexion à 15 minutes de non-activité. Si votre ordinateur est inactif depuis plus de 15 minutes, vous devrez vous reconnecter au Système.

8. Expiration de l'Utilisateur

Si vous ne vous êtes pas connecté au système depuis 90 jours, votre compte Utilisateur expire et vous devez demander à votre Administrateur de le réinitialiser.

9. Nouvel utilisateur ou mot de passe réinitialisé

Pour un nouvel utilisateur à qui un mot de passe temporaire a été envoyé, ou pour un utilisateur ayant demandé une réinitialisation de mot de passe et ayant reçu un nouveau mot de passe temporaire, l'utilisateur doit se connecter avec le mot de passe temporaire dans les 24 heures. Après cela, celui-ci expire et l'Administrateur doit le réinitialiser.