bookassist®
technology & online strategy for hotels

Implémentation de PCI DSS au sein de Bookassist
Document Version 2.0

A propos de la PCI DSS

Les standards de sécurité pour le paiement en ligne répondent à l'appellation PCI DSS (Payment Card Industry Data Security Standards), et représentent les meilleures pratiques à adopter pour le paiement en ligne par carte de crédit Visa & Mastercard. Ces standards aident Bookassist et l'hôtelier à se protéger contre les conséquences des accès frauduleux aux cartes de crédit des clients.
Alors que Bookassist fournit tout le nécessaire pour permettre aux hôtels d'implémenter des standards de sécurité, il retourne de la responsabilité des hôtels utilisant le Système d'Administration de Bookassist de s'assurer que leur utilisation du système soit en accord avec les critères PCI. Les hôtels doivent donc nommer un Administrateur pour le Système d'Administration de Bookassist, qui sera responsable de contrôler les accès des autres utilisateurs de l'hôtel.

Merci de noter qu'en utilisant le Système d'Administration de Bookassist, vous acceptez les Conditions exposées ci-dessous

Conditions
1. Protection des données et Normes Payment Card Industry (PCI)

Bookassist doit dûment être conforme à toutes les normes de la Loi de Protection des Données (Data Protection Act) de 1988 (énoncées dans cette clause), incluant le respect de celles ci : a) Les principes Data Protection établis dans la Loi ; b) Demandes de données sujet pour l'accès au données ; et c) Les critères concernant l'enregistrement des utilisateurs. Toute divulgation ou transfert de données par Bookassist à des personnes autorisées avec un accord spécifique de sites tiers pour le faire, doivent être conformes à la Législation Data Protection. Dans cette clause, « Donnée » désigne toute information fournie ou qui sera fournie à Bookassist ou à l'Hôtelier par un site tiers incluant toute application, réservation ou donnée de transaction impliquant des détails de carte de paiement ou toute autre donnée du genre.
Bookassist fournit tous les efforts nécessaires pour être entièrement conforme aux conditions posées par les Data Security Standards de la Payment Card Industry (PCI DSS) pour les procédures de paiement en ligne.

L'Hôtelier est entièrement responsable de la bonne application des critères PCI DSS implémentés par Bookassist. Il est également responsable quant à l'administration des utilisateurs locaux ayant un accès au Système d'Administration de Bookassist, et à la protection des noms d'utilisateurs et mots de passe du système, en particulier au contrôle des utilisateurs ayant un accès autorisé aux détails bancaires des clients. L'hôtelier garantit surtout qu'il :
adhère aux normes de sécurité PCI DSS
reconnaît sa part de responsabilité dans la sécurisation des données du Porteur de la Carte
reconnaît que les données du Porteur doivent seulement être utilisées pour aider à compléter la transaction, pour les besoins d'un programme de fidélité, pour les besoins d'un service de contrôle des fraudes ou pour des usages spécifiquement demandés par la Loi
fera preuve de coopération en fournissant à un représentant de la PCI un examen de sécurité minutieux après une intrusion, ou à un tiers nommé par la PCI.
Reconnaît que ces obligations pour sauvegarder la confidentialité des données du Porteur doivent durer tout au long des accords contractuels qui le lient à Bookassist
Toute violation de standards, procédures ou instructions générales établies, conformément à cette politique, devra être présentée au management de l'Hôtelier qui décidera d'une action appropriée. Cela peut aboutir à une sanction disciplinaire, incluant le licenciement et/ou des poursuites judiciaires.

2. Spécificités

Accès nécessaire
L'accès au système à ce niveau particulier doit être donné uniquement aux utilisateurs qui ont spécifiquement besoin d'un tel accès pour exercer leurs fonctions.

Accès et Restrictions des Données
L'accès doit uniquement être donné lorsqu'autorisé par le client/manager de l'hôtel ou responsable des réservations. Les données du Porteur de la carte de crédit ne sont consultables que jusqu'à un mois après la date de départ de la réservation. Après cette date, les données seront automatiquement supprimées par le système de Bookassist et ne pourront pas être récupérées.

Logins Individuels
Les Logins doivent être uniques pour chaque utilisateur. Les utilisateurs ne doivent pas partager leur compte avec qui que ce soit.

Utilisateurs inactifs
Les Logins doivent être immédiatement supprimés s'ils ne servent plus.

Nouveaux Utilisateurs
Lorsque le compte pour le Système d'Administration de Bookassist est créé, l'utilisateur doit lire, comprendre et accepter les conditions listées plus haut.

Notes Explicatives sur la politique des mots de passe

Les standards PCI impliquent que les mots de passe que vous utilisez sur le Système d'Administration de Bookassist doivent respecter quelques règles. La procédure «login» sur le Système garantit que les standards PCI sont respectés. La vérification des identifiants valide le nom d'utilisateur et le mot de passe, et, si erreur, affiche des messages clairs à l'écran sur ce qui est erroné et comment corriger.
Mots de Passe fiables
Sélectionnez des mots de passe fiables avec ces caractéristiques:

- Utilisez à la fois des majuscules et des minuscules, et des chiffres ou des signes de ponctuation
- N'utilisez pas des informations personnelles ou des mots du dictionnaire
- Ne partagez pas votre mot de passe
- N'inscrivez pas votre mot de passe et ne le gardez pas en mémoire en ligne.

Durée de validité du mot de passe
Tous les 90 jours, le Système vous demande de changer votre mot de passe. Des instructions claires vous guident dans la procédure.

Format du mot de passe
Le mot de passe doit comporter au minimum 7 caractères, avec un minimum d'un chiffre et d'un caractère alphabétique. Si vous changez votre mot de passe et qu'il ne correspond pas à cela, alors un message apparaît à l'écran, expliquant ce que vous devez modifier pour rendre votre mot de passe valide.

Historique des mots de passe
Lorsque vous changez votre mot de passe, le Système vérifie que ce dernier ne corresponde pas à l'un de vos 4 derniers mots de passe.

Tentatives d'identification
Si vous vous identifiez et que vous entrez un mauvais mot de passe, vous avez un total de 6 tentatives avant que votre session soit verrouillée. Si cela se produit, vous devez demander à l'Administrateur de réinitialiser le mot de passe et attendre 30 minutes avant de vous identifier.

Délai de session verrouillée
Si votre session a été verrouillée à cause de 6 mots de passe erronés, vous devez attendre 30 minutes avant de vous reconnecter, et cela même si l'Administrateur a réinitialisé votre mot de passe.

Session inactive
PCI nous impose de limiter une session à 15 minutes d'inactivité. Donc si votre ordinateur est inactif pendant plus de 15 minutes, vous devez vous ré-identifier sur le Système.

Utilisateur expiré
Si vous ne sous êtes pas connecté au Système pendant 90 jours, votre nom d'utilisateur expire et vous devez demander à l'Administrateur de le réinitialiser.

Nouvel utilisateur ou mot de passe réinitialisé
Pour un nouvel utilisateur à qui on a envoyé un mot de passe temporaire, ou pour un mot de passe réinitialisé, l'utilisateur doit s'identifier avec le mot de passe temporaire dans les 24 heures. Après ce délai, il aura expiré et l'Administrateur devra le réinitialiser.

