bookassist®
technology & online strategy for hotels

Implementação dos PCI DSS na Bookassist
Versão do documento: 2.0

Sobre os PCI DSS

Os padrões de segurança para pagamentos on-line são conhecidos como PCI DSS – *Payment Card Industry Data Security Standards* (normativa de segurança de dados do setor de "cartões para pagamento"), e representam os melhores requisitos do procedimento para o processamento on-line de cartão de crédito Visa e MasterCard. Estes padrões ajudam a proteger você e a Bookassist das consequências de um acesso fraudulento aos cartões de crédito do cliente.

Embora a Bookassist ofereça todas as funções necessárias para ajudar os hotéis a implementar estes padrões de segurança, é responsabilidade dos próprios hotéis usar o Sistema de Administração da Bookassist para garantir que o uso do sistema seja realizado conforme os requisitos PCI. Assim, os hotéis devem determinar um administrador do sistema de administração da Bookassist, que será responsável pelo controle do acesso de outros usuários no hotel.

Lembre-se de que ao usar o sistema de administração da Bookassist, você confirma sua aceitação dos termos e condições apresentados aqui.

Termos e condições

1. Proteção de dados e requisitos do setor de cartões para pagamento (PCI)

A Bookassist deve cumprir estritamente todos os requisitos relevantes da Lei de Proteção de Dados de 1988 (doravante, nesta cláusula, LPD), inclusive de acordo com o seguinte: a) Princípios de proteção de dados estabelecidos na LPD; b) Pedidos de pessoas registradas para acesso a dados seguros; e c) Os requisitos relativos à inscrição de usuários. Qualquer revelação ou transferência de dados por parte da Bookassist a pessoas aprovadas com consentimento específico de terceiros para tanto só poderá realizar-se em conformidade com a legislação de proteção de dados aplicável. Nesta cláusula, a palavra "dados" compreende todas e quaisquer informações que foram fornecidas ou serão fornecidas à Bookassist ou ao provedor do alojamento por parte de terceiros, inclusive em qualquer aplicação, reserva e dados de transação relativos a detalhes de pagamento com cartão de crédito ou quaisquer outros dados.
A Bookassist empenha-se em cumprir estritamente as condições estabelecidas pelos Padrões de Segurança de Dados do Setor de Cartões para Pagamento (PCI DSS) para o processamento de pagamentos on-line.

O provedor do alojamento é totalmente responsável pela operação em conformidade com os requisitos PCI DSS implementados pela Bookassist, no que se refere a: administração de usuários locais com acesso ao sistema de administração de hotel da Bookassist, proteção de nomes de usuário e senhas para acesso ao sistema e, particularmente, controle sobre a autorização de acesso garantido dos usuários, e detalhes dos cartões dos clientes. Especialmente, o provedor do alojamento garante que:

- se adere aos requisitos de segurança PCI DSS;
- reconhece sua responsabilidade para assegurar os dados do titular do cartão;
- reconhece que os dados do titular do cartão só devem ser usados para ajudar a conclusão de uma transação, baseando-se em um programa de lealdade, fornecendo um serviço de controle de fraude ou para usos especificamente requeridos pela lei;
- prestará cooperação e acesso para realizar uma revisão de segurança completa, após uma intrusão de segurança, a um representante do setor de cartões para pagamento, ou setor de cartões de pagamento aprovado por terceiros;
- reconhece que tais obrigações para salvaguardar a confidencialidade dos dados do titular do cartão devem prevalecer ao término de quaisquer outros acordos contratuais com a Bookassist.

Qualquer violação dos padrões, diretrizes ou procedimentos estabelecidos de acordo com esta política deve ser submetida à gerência do provedor do alojamento para que tome a ação apropriada. Isto poderia resultar em ação disciplinar, inclusive demissão ou interrupção de serviço e/ou processo legal.

2. Particularidades

Acesso com base à necessidade de conhecimento
O acesso ao sistema em um nível particular só deve aplicar-se aos usuários que precisem do acesso especificamente no nível determinado para desempenharem seu trabalho.

Acesso e restrições de dados
O acesso só deve ser autorizado pelo cliente/gerente do hotel ou gerente de reservas.
Os dados do cliente titular de um cartão só podem ser visualizados no prazo de até um mês após a data de realização do registro do cliente. Após este prazo, os dados são apagados automaticamente do sistema da Bookassist e já não poderão ser recuperados.

Logins individuais

Os *logins* devem ser exclusivos para cada usuário. Os usuários não podem compartilhar seu *login* com ninguém.

Usuários inativos
Os *logins* serão apagados imediatamente para o pessoal que já não o necessita, ou que deixou o hotel.

Novos usuários
Quando *logins* são instalados no sistema de administração da Bookassist, o usuário está obrigado a ler, entender e aceitar as condições mencionadas acima.

Notas explicativas da política de senhas

Os padrões PCI significam que as senhas utilizadas no sistema de administração da Bookassist devem atender a um conjunto particular de regras. O procedimento de *login* no sistema garante que os padrões PCI sejam adequados. A verificação do *login* da Bookassists validará o nome do usuário e a senha e, no caso de erros, aparecerão mensagens claras na tela para explicar o que está errado e como corrigir tais erros.

Senhas seguras
Selecione senhas seguras com estas características:

- use tanto caracteres em minúsculas como maiúsculas, além de dígitos ou sinais de pontuação
- não use nenhuma informação pessoal ou palavras de uso comum ou que estejam dicionarizadas
- não compartilhe uma senha com ninguém
- não escreva uma senha nem a armazene on-line.

Duração da senha
A cada 90 dias, o sistema exige que você mude sua senha. Você receberá instruções claras durante este processo.

Formato da senha
A extensão da senha deve ser de no mínimo 7 caracteres, com pelo menos 1 número e 1 letra do alfabeto. Ao modificar sua senha, se você não observar estes requisitos, aparecerá uma mensagem na tela para informar sobre o que você deve fazer para criar uma senha válida.

Histórico da senha
Quando você modificar sua senha, o sistema realiza uma verificação para confirmar que esta não corresponde a uma de suas 4 últimas senhas.

Tentativas de login
Se você introduzir uma senha errada ao realizar o *login*, terá um total de 6 tentativas antes de bloquear-se. Se isto acontecer, você deverá consultar seu administrador para reativar a senha e esperar 30 minutos para realizar o *login* novamente.

Tempo de bloqueio
Se a sua entrada no sistema for impedida porque você introduziu uma senha errada 6 vezes, neste caso você deve esperar 30 minutos, e só poderá realizar o *login* novamente depois que o administrador reativar sua senha.

Intervalo de sessão
O PCI exige realizar um novo *login* após 15 minutos de inatividade em uma sessão. Por tanto, se seu computador ficar inativo por mais de 15 minutos, você deverá realizar novamente o *login* no sistema.

Usuário cancelado
Se você não realizar o *login* no sistema por mais de 90 dias, seu nome de usuário será cancelado e será necessário consultar o administrador para reativá-lo.

Novo usuário ou senha reativada
Para um novo usuário que recebe uma senha temporária, ou para um usuário que solicitou a reativação de uma senha e recebeu uma nova senha temporária, o usuário deve realizar o *login* com a senha temporária durante 24 horas. Depois deste prazo, ela expirará e o administrador deve reativá-la.

