bookassist®
technology & online strategy for hotels

Bookassist Implementierung von PCI DSS
Dokument Version 2.0

Über PCI DSS

Die Sicherheitsstandards für Onlinezahlung werden PCI DSS (Payment Card Industry Data Security Standards) genannt und beinhalten die besten Möglichkeiten von Visa & Mastercard für Online Kreditkartenzahlungen. Diese Standards dienen Ihnen und Bookassist zum Schutz vor den Konsequenzen von in betrügerischer Absicht durchgeführten Zugriffen auf die Kundenkreditkartendaten der Gäste.

Obwohl Bookassist alle nötigen Einstellungen zur Verfügung stellt, die dem Hotel helfen sollen die Sicherheitsstandards umzusetzen, liegt es in der Verantwortung des Hotels, das Bookassist Administrationssystem zu benutzen, um sicher zu gehen, dass das System den PCI-Ansprüchen entspricht. Die Hotels müssen für das Bookassist Administrationssystem einen Administrator einsetzen, welcher für die Kontrolle der Zugriffe von anderen Benutzern des Hotels verantwortlich ist.

Beachten Sie bitte, dass Sie beim benutzen des Bookassist Administrationssystems, zustimmen die unten angeführten Geschäftsbedingungen durchgelesen und bestätigt haben.

Geschäftsbedingungen

1. Datenschutz und Payment Card Inudstrie (PCI) Anforderungen

Bookassist muss ordnungsgemäß alle relevanten Anforderungen für das Datenschutzgesetz 1988(in diesem Fall das Gesetz) zur Verfügung stellen. Dies beinhaltet die Einhaltung von: a) den, in dem Gesetz veröffentlichten, Datenschutzprinzipien b) Anfragen an die Datenobjekte für den Zugriff auf die gespeicherten Daten. c) Die Anforderungen für die Registrierung der Benutzer. Jede Offenlegung von Daten durch Bookassist zu Personen, mit speziellem Einverständnis der Kunden, von 3.en Parteien muss in der vorgeschriebenen Art und Weise der Data Protection Legislation durchgeführt werden. In diesem Fall bedeutet „Daten“ jede Information welche zur Verfügung gestellt wurde, oder, Bookassist oder dem Hotelbesitzer von einer 3.en Partei zur Verfügung gestellt wird, beinhaltet alle Applikationen, Reservationen und Transaktionen Daten hinsichtlich Kreditkartenzahlungsdetails oder anderer, gleichartiger Daten.
Bookassist scheut keinen Arbeitsaufwand um die Bedingungen, die in den Payment Card Industry's Data Security Standards (PCI DSS) für die Onlinezahlung niedergeschrieben sind, zu erfüllen.

Der Hotelbesitzer ist vollständig verantwortlich für die weiteren Einsatz der PCI DSS Bedingungen die von Bookassist zur Verfügung gestellt wurden, **in Hinsicht der Administration von lokalen Benutzern mit Zugriff auf die Bookassist Hoteladministrations, Schutz der Benutzernamen und Passwörter für das System und im speziellen Kontrolle über die Zugriffserlaubnisse zu den Kreditkartendetails von Gästen. Im speziellen garantiert der Hotelbesitzer das:**

- er die PCI DSS Sicherheitsbedingungen befolgen wird
- die Verantwortung für die Sicherheit der Informationen von den Kartenbesitzern bestätigt ist
- die Kreditkartenbesitzerdaten nur als Hilfenahme für das Vervollständigen von Transaktionen, zur Hilfestellung bei einem Treueprogramm, zur Erstellung eines Betrugskontrollenservice oder für spezielle, vom Gesetz verlangte, Dienste verwendet werden.
- Er die vollständige Zusammenarbeit und den Zugriff für die Abwicklung von Sicherheitsüberwachungen nach einem Einbruch in die Zahlung über ein repräsentatives Kreditkarteninstitut, oder einer Zahlung von einem 3.en Parteien Kreditkarteninstitut, versichert.
- Er zustimmt, dass die Zustimmungen zu den Absicherungen der Geheimhaltung der Informationen des Kartenbesitzers, auch nach der Beendigung jedweder Verträge mit Bookassist bestehen bleibt.

Jede Missachtung der Standards, Prozeduren oder genannte Richtliien, welche auf diese Vorschriften aufbauen, wird dem Beherbergungsbetrieb zur Kenntnis gebracht, um geeignete Maßnahmen einzuleiten.Dies kann auch zu disziplinären Maßnahmen führen, einschließlich Unterbrechung oder Beendigung des Services und / oder der Einleitung rechlicher Schritte.

2. Details

Zugriff auf einer Vertrauensbasis
Zugriff zu dem System ab einem bestimmten Level, soll nur jenen Benutzern gegeben werden, welche diesen Zugriff wirklich benötigen um Ihren Job durchführen zu können.

Zugriff und Datenrestriktionen
Zugriffserlaubnisse sollen nur dann vergeben werden, wenn dies vom Kunden/Hotelmanager oder Reservierungsmanager angeordnet wurde. Die Kreditkarteninformationen des Kunden können nur bis zu einem Monat,

nach der Abreise des Kunden, angesehen werden. Nach diesem Zeitpunkt, werden die Informationen automatisch vom Bookassist Server gelöscht und können nicht erneuert werden.

Individuelle Logins
Logins müssen für jeden Benutzer einzigartig sein. Benutzer dürfen Ihren Login nicht mit anderen Personen teilen.

Inaktive Benutzer
Logins von Mitarbeitern die diesen nicht mehr benötigen oder das Hotel verlassen haben, müssen unverzüglich gelöscht werden.

Neue Benutzer
Wenn die Logins für das Bookassist Administrationssystem aufgesetzt wurden, ist der Benutzer verpflichten die oben angeführten Konditionen gelesen und verstanden zu haben.

Erklärende Bemerkungen für die Passwortrichtlinien

PCI Standards bedeuten, dass Ihr Passwort, welches Sie für das Bookassist Administrationssystem benutzen, einigen Regeln entsprechen muss. Die Loginprozedur des Systems stellt sicher dass die PCI Standards eingehalten werden. Das Bookassist Login überprüft die Gültigkeit Ihres Benutzernamen und Passworts und bei auftretenden Fehlern erscheint eine deutliche Mitteilungen am Bildschirm, welche Erklärt was Fehlgeschlagen ist und wie man dies beheben kann.

Sichere Passwörter
Durch diese Eigenschaften wählen Sie ein sicheres Passwort

- Benutzen Sie Groß- und Kleinbuchstaben, sowie Ziffernfolgen oder Satzzeichen.
- Benutzen Sie keine persönlichen Informationen oder Wörter die im Alltäglichen Einsatz sind oder im Wörterbuch gefunden werden können.
- Teilen Sie ein Passwort NIE mit jemand anderem.
- Schreiben Sie das Passwort nicht nieder oder bewahren Sie es online auf.

Passwort Laufzeit
Alle 90 Tage verlangt das System von Ihnen, Ihr Passwort zu ändern. Klare Hilfemitteilung leiten Sie durch diesen Ablauf.

Passwort Format
Das Passwort muss mindestens 7 Zeichen lang sein, mit einem Minimum von 1 Zahl und 1 Buchstaben. Wenn Sie Ihr Passwort ändern, und es nicht diesen Anforderungen entspricht, erscheint eine deutliche Mitteilung am Bildschirm, welche Ihnen mitteilt, was nötig ist um ein gültiges Passwort wählen zu können.

Passwort Geschichte
Wenn Sie Ihr Passwort ändern, überprüft das System ob es keines der letzten 4, von Ihnen gewählten, Passwörtern entspricht.

Login Versuche
Wenn Sie versuchen sich einzuloggen und das falsche Passwort verwenden, haben Sie 6 Versuche bevor Sie aus dem System ausgesperrt werden. Wenn dies passiert, setzen Sie sich mit Ihrem Administrator in Verbindung, damit dieser Ihr Passwort zurücksetzt. Warten Sie 30 Minuten und Login sich ein.

Lockout Zeit
Wenn Sie aus dem System ausgesperrt wurden, weil Sie das falsche Passwort öfter als 6 mal falsch eingegeben haben, müssen sie 30 Minuten warten, bevor Sie sich erneut einloggen können, auch wenn Ihr Passwort bereits von Ihrem Administrator zurückgesetzt wurde.

Timeout der Sitzung
Aufgrund von PCI müssen wir die Loginsitzung auf 15 Minuten Inaktivität begrenzen. Wenn Ihr Computer für 15 Minuten Stillstand, müssen Sie sich erneut in das System einloggen.

Benutzer ist ausgelaufen
Wenn Sie sich innerhalb von 90 Tagen nicht in das System eingeloggt haben, läuft Ihr Benutzer aus und Sie müssen sich an Ihren Administrator wenden um Ihn zurückzusetzen.

Neue Benutzer oder zurücksetzen eines Passworts
Neue Benutzer die ein zeitlich begrenztes Passwort erhalten haben, oder bereits bestehende Benutzer, welche ihr Passwort zurücksetzen haben lassen und bereits ein neues zeitlich begrenztes Passwort erhalten haben, müssen sich innerhalb von 24 Stunden mit dem zeitlich begrenzten Passwort einloggen. Wenn diese Frist verstreicht, muss der Administrator es erneut zurücksetzen.

