bookassist®
technology & online strategy for hotels

Conformita' di Bookassist al Protocollo PCI DSS
Versione Documento 2.0

Riguardo il protocollo PCI DSS

Gli standard di sicurezza per i pagamenti online noti come PCI DSS (Payment Card Industry Data Security Standards) rappresentano il miglior sistema di protezione elaborato da Visa e Mastercard per garantire la sicurezza di ogni transazione che viene effettuata online mediante carta di credito. Questi standard di sicurezza garantiscono sia l'hotel che Bookassist in caso di accesso non autorizzato alle carte di credito dei clienti.

Bookassist garantisce tutte le condizioni indispensabili per permettere agli hotel l'adozione di questi standard di sicurezza. Tuttavia, e' responsabilita' degli hotel che utilizzano il Sistema di Amministrazione di Bookassist assicurarsi che l'utilizzo di tale Sistema sia conforme ai requisiti PCI.
Si invita dunque gli hotel a nominare un Amministratore per il Sistema di Amministrazione di Bookassist, il quale sara' responsabile dell'accesso di altri utenti all'interno dell'hotel.

Si prega di notare che l'utilizzo del Sistema di Amministrazione di Bookassist equivale all'accettazione dei Termini e Condizioni elencati di seguito.

Termini e Condizioni

1. Protezione dei Dati e Requisiti PCI
Bookassist si impegna a conformarsi debitamente a tutti i requisiti rilevanti del Data Protection Act 1988 (in questo documento "Act") inclusa l'accettazione: a) dei principi del Data Protection stabiliti nell'Act b) delle richieste da parte dei soggetti titolari dei Data contenuti nello stesso c) dei requisiti relativi alla registrazione degli utenti. Ogni divulgazione o trasferimento dei dati da parte di Bookassist a persone la cui approvazione a fare cio' sia stata rilasciata sulla base del consenso specifico fornito da terzi dovra' in ogni modo essere conforme alla legislazione sul Data Protection. In questo contesto si intende per "Data" qualsiasi informazione che e' stata fornita o sara' fornita a Bookassist o alla struttura ricettiva da terzi inclusi i dati relativi a domande, prenotazioni e transazioni nel rispetto degli estremi di pagamento della carta di credito o simili.
Bookassist si impegna a conformarsi in pieno alle condizioni stabilite dai Payment Card Industry's Data Security Standards (PCI DSS) per il trattamento dei pagamenti online.

La struttura ricettiva e' pienamente responsabile della corretta messa in funzione dei i requisiti PCI DSS implementati da Bookassist e relativi all'amministrazione degli utenti locali con accesso al Sistema di Amministrazione Hotel di Bookassist, della protezione di ciascun username and password presenti nel Sistema ed in particolare del controllo sugli utenti che hanno accesso agli estremi delle carte di credito dei clienti. In particolare, la struttura ricettiva

- si impegna a rispettare i requisiti di sicurezza PCI DSS;
- riconosce la propria responsabilita' riguardo la sicurezza dei dati del titolare della carta di credito;
- si impegna ad utilizzare i dati del titolare della carta di credito soltanto per i fini relativi al completamento della transazione, il mantenimento di un programma loyalty, la fornitura di un servizio di controllo anti-frode o per gli usi stabiliti dalla legge;
- nell'eventualita' di un'intrusione, si impegna a fornire piena cooperazione ed accesso nella conduzione di un'indagine sulla sicurezza ad un rappresentante dell'industria della carta di credito;
- si impegna a garantire gli obblighi relativi alla salvaguardia della confidenzialita' dei dati del titolare della carta di credito anche in seguito alla cessazione di ogni accordo contrattuale con Bookassist.

Qualsiasi violazione degli standard, delle procedure o delle linee guida stabilite in conformita' a questa procedura sara' portata a conoscenza dei responsabili della struttura ricettiva per un'azione appropriata. Questo potrebbe risultare in un'azione disciplinare. incluso il licenziamento o la cessazione del servizio e/o la prosecuzione legale.

2. Specifiche
Accesso su base di stretta necessita' (need-to-know)
L'accesso ad uno specifico livello del sistema dovrebbe essere garantito soltanto agli utenti che necessitano dell'accesso a quel livello specifico per eseguire il proprio lavoro.

Accesso e Restrizioni dei Dati

© Bookassist. All Rights Reserved. Bookassist is a registered trademark.

L’accesso dovrebbe essere garantito soltanto in caso di autorizzazione da parte del cliente o dell’hotel/reservations manager
I dati del cliente titolare della carta di credito potranno essere visionati soltanto fino ad un mese dalla data di partenza relativa alla prenotazione. Scaduto tale termine, i dati verranno automaticamente cancellati dal Sistema di Bookassist e non potranno piu’ essere recuperati.

Login Individuali
Un unico login dovra’ essere configurato per ogni singolo utente. Gli utenti non dovranno condividere i loro login con nessun altro.

Utenti Inattivi
I login per coloro tra i membri dello staff che non ne hanno piu’ necessita’ o che hanno lasciato l’hotel dovranno essere prontamente cancellati.

Nuovi Utenti
Una predisposti i login nel Sistema di Amministrazione Bookassist, l’utente sara’ tenuto a leggere, comprendere ed accettare le condizioni sopra elencate.

Nota Esplicativa sulle Norme Relative alle Password

Gli standard PCI richiedono che le password utilizzate nel Sistema di Amministrazione di Bookassist debbano rispettare un certo numero di regole. La procedura di login del Sistema assicura il rispetto degli standard PCI. Il controllo dei login da parte di Bookassist si occupa della convalida di username e password e, in caso di errori, fornisce chiari messaggi su schermo che illustrano il tipo di errore e la successiva correzione.

Password Sicure
Una password sicura:

- fa uso sia di lettere maiuscole che minuscole, cosi’ come numeri e punteggiatura
- non contiene informazioni personali o parole di uso comune o trovate sul dizionario
- non viene trascritta o tenuta online.

Durata della Password
Ogni 90 giorni, il Sistema richiede di cambiare la propria password. L’utente sara’ guidato attraverso questo processo per mezzo di istruzioni chiare e semplici da comprendere.

Formato della Password
La password deve contenere un minimo di 7 caratteri, con almeno un numero ed un carattere alfabetico. Nel caso in cui la nuova password non rispetti questi requisiti, verra’ visualizzato un messaggio sullo schermo, con spiegazioni chiare su come rendere la password valida.

Cronologia Password
Quando viene cambiata una password, il Sistema esegue un controllo per verificare che la nuova password non sia uguale ad una delle ultime quattro.

Tentativi di Login
Si hanno a disposizione 6 tentativi per effettuare il login con la password corretta, falliti i quali l’accesso verra’ negato e sara’ necessario attendere 30 minuti prima di poter effettuare un nuovo login, anche nel caso in cui l’Amministratore resetti la password.

Accesso Negato
Nel caso sia impossibile accedere al Sistema a causa di 6 tentativi di login falliti (a causa dell’inserimento di una password non corretta), si dovra’ attendere 30 minuti prima di poter accedere di nuovo an Sistema, anche nel caso in cui l’Amministratore resetti la password.
If you were locked out of the System because you entered the wrong password 6 times, then you have to wait 30 minutes before you can log back in, even after the Administrator reset your password.

Sospensione della Sessione
Gli standard PCI richiedono di limitare le sessioni di login a 15 minuti di non-attivita’. Nel caso in cui il computer rimanga inattivo per piu’ di 15 minuti, si dovra’ nuovamente effettuare il login.

Utente Scaduto
Nel caso in cui l’utente non abbia effettuato il login per una durata consecutiva di 90 giorni, lo stesso sara’ considerato scaduto e sara’ necessario rivolgersi all’Amministratore per un’operazione di reset.

Nuovo Utente o Reset della Password
Nel caso in cui una password temporanea sia stata inviata ad un nuovo utente oppure ad un utente che abbia richiesto il reset della propria password, lo stesso dovra’ effettuare il login con la suddetta password temporanea nell’arco della successive 24 ore. Trascorse le quali, la password verra’ considerata scaduta e l’Amministratore dovra’ effettuare una operazione di reset.

© Bookassist. All Rights Reserved. Bookassist is a registered trademark.