bookassist
technology & online marketing for hotels

Bookassist Implementation of PCI DSS
Document Version 2.0

About PCI DSS

The security standards for payments online are known as PCI DSS (Payment Card Industry Data Security Standards), representing best practice requirements from Visa & Mastercard for online credit card processing. These standards help protect you and Bookassist from the consequences of fraudulent access to customer credit cards.

While Bookassist provides all the required features to help hotels implement this security standard, it is the responsibility of hotels using the Bookassist Administration System to ensure that their use of the System meets PCI requirements. Hotels therefore need to appoint an Administrator for the Bookassist Administration System who will be responsible for controlling the access of other users in the hotel.

Note that by using the Bookassist Administration System, you are acknowledging your acceptance of the Terms & Conditions outlined here.

Terms & Conditions

1. Data Protection and Payment Card Industry (PCI) Requirements

Bookassist shall duly comply with all relevant requirements of the Data Protection Act 1988 (in this clause the Act) including compliance with the following: a) The Data Protection principles established in the Act; b) Requests from Data subjects for access to data held by it; and c) The requirements relating to the registration of users. Any disclosure or transfer of data by Bookassist to persons approved with specific consent from third parties to do so shall be in a manner compliant with applicable Data Protection Legislation. In this clause “Data” means all and any information which has been provided or will be provided to Bookassist or the Accommodation Provider by a third party including any application, reservation and transaction data in respect of credit card payment details or other such data.
Bookassist makes every effort to fully comply with the conditions laid down by the Payment Card Industry’s Data Security Standards (PCI DSS) for the processing of online payments.

The Accommodation Provider is fully responsible for the proper operation of PCI DSS requirements implemented by Bookassist with regard to administration of local users with access to the Bookassist Hotel Administration system, protection of usernames and passwords for the system, and in particular control over users granted access permission to credit card details of customers. In particular the Accommodation Provider warrants that it

- will adhere to the PCI DSS security requirements;
- acknowledges their responsibility for securing the Card Holder data;
- acknowledges that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law;
- will provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party;
- acknowledges that these obligations to safeguard the confidentiality of the Card Holder data shall survive the termination of any other contractual agreements with Bookassist.

Any violation of standards, procedures or guidelines established pursuant to this policy shall be presented to the management of the Accommodation Provider for appropriate action. This could result in disciplinary action, including dismissal or discontinuation of service and/or legal prosecution.

2. Specifics

Access on a need-to-know basis
Access to the system at a particular level should only be given to those users who specifically need access at that level to perform their job.

Access and Data Restrictions
Access should only be given where authorised by the client/hotel manager or reservations manager.

Customer cardholder data can only be viewed for up to one month after the customer's booking departure date. After that, the data is automatically deleted from the Bookassist system and cannot be retrieved.

Individual Logins
Logins must be unique for each user. Users may not share their login with anyone else.

Inactive Users
Logins should be immediately deleted for staff that no longer need it, or have left the hotel.

New Users
When logins are set up for the Bookassist Admin system, the user is obliged to read, understand and accept the conditions listed above.

Explanatory Notes on Password policy

PCI standards mean that passwords you use on the Bookassist Administration System must meet a particular set of rules. The login procedure on the System ensures that the PCI standards are met. Bookassist's login checking will validate username and password and for errors will give clear messages on screen explaining what's wrong and how to correct them.

Strong Passwords
Select strong passwords with these characteristics:
- use both upper and lower case characters, and digits or punctuation characters
- do not use personal information or words in common usage or found in a dictionary
- do not share a password with anyone
- do not write down a password or store it online.

Password age
Every 90 days, the System requires you to change your password. Clear instructions take you through this process.

Password Format
Password length must be a minimum of 7 characters , with a minimum of 1 number and 1 alphabet character. If you change your password and it doesn't meet these requirements, then a screen message is displayed, telling you what to do to make the password valid.

Password History
When you change your password, the System checks to make sure it doesn't match any of your last 4 passwords.

Login attempts
If you're logging in and you enter the wrong password, you have a total of 6 attempts before you are locked out. If this happens, you should ask your Administrator to reset the password and wait 30 minutes to login again.

Lockout time
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.

Session Timeout
PCI requires us to limit a login session to 15 minutes of non-activity. So if your computer has been idle for more than 15 minutes, you'll have to log in again to the System.

User expired
If you haven't logged in to the System in 90 days, your user expires and you need to ask your Administrator to reset it.

New User or Password Reset
For a new user who's been sent a temporary password, or for a user who requested a password reset and has been sent a new temporary password, the user must log in with the temporary password within 24 hours. After that, it has expired and the Administrator must reset it.