Bookassist®

Bookassist Extranet Policy

Last update: 25 May 2018

This policy includes:

1) Terms & Conditions for the use of the Bookassist Administration System ("System")
2) Data Protection Information for Employees / Authorised Personnel accessing the System and or the Bookassist Content Management System ("CMS")
3) Explanatory Notes on Password policy for the use of the System

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

The System provides access to personal data based on the contractual obligations laid down in the Bookassist Contract with the Accommodation Provider and in accordance with the Bookassist Data Processing and Security Terms (https://bookassist.org/dp).

Terms & Conditions for the use of the Bookassist Administration System ("System")

1. PCI DSS (Payment Card Industry Data Security Standards) Requirements

a) While 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 use of personal data provided on the System in accordance with the relevant data protection legislation.

b) The Accommodation Provider must appoint an Administrator for the System who will be responsible for controlling the access of other employees and or authorised personnel to the System ("Users").

c) The Accommodation Provider is fully responsible for the proper operation of PCI DSS requirements implemented by Bookassist with regard to administration of Users with access to the System, protection of usernames and passwords for the system, and in particular control over Users granted access to credit card details of the Card Holder. 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.

d) 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. 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.

3. Access and Data Restrictions

a) Access should only be given where authorised by the Accommodation Provider.

b) Customer credit card data can only be viewed for up to one month after the booking departure date. After that, the data is automatically deleted from the Bookassist system and cannot be retrieved.

c) All other Customer Personal Data is anonymized 12 months after departure date.

4. Individual Logins

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

5. Inactive Users

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

6. New Users

When logins are set up for the System, the user is obliged to read, understand and accept the conditions listed above.

Data Protection Information for Employees/ Authorised Personnel accessing the System and or the Content Management System ("CMS")

1. Information Collected about Employees/ Authorised Personnel ("Users") accessing the System or the CMS and Why it is Collected and Processed

a) Users that access the System or the CMS are required to provide name, email address, phone. Furthermore, the System and the CMS record log information of all accesses and activities.

b) Such collection and processing of data is necessary for the functionality of the System and the CMS and to analyse problems to enable us to respond to issues.

2. How the User data may be used and Who has access

The User data shall be used to support the functioning of the System and the CMS. The Accommodation Provider may request access to User data. Please contact the relevant Accommodation Provider for details on how they may use this User data. Please note that if the Accommodation Provider requested the user data, the Accommodation Provider may retain access to it for a different retention period.

3. Rights of the User

Users have the right to request access to, rectification and erasure of their data, as well as the right to data portability and the right to lodge a complaint with the relevant supervisory authority in line with the relevant data protection requirements.

4. Retention

All such data listed in section 1 shall be retained by Bookassist for two years after the user expiry date.

5. Contact

You may email the Bookassist Data Protection contact at dpo@bookassist.com if you require further information or would like to exercise your rights.

Explanatory Notes on Password policy for the use of the System

PCI standards mean that passwords you use on the 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.

1. 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.

2. Password age

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

3. 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 does not meet these requirements, then a screen message is displayed, telling you what to do to make the password valid.

4. Password History

When you change your password, the System checks to make sure it does not match any of your last 4 passwords.

5. Login attempts

If you are 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.

6. 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.

7. Session Timeout

PCI requires us to limit a login session to 15 minutes of non-activity. If your computer has been idle for more than 15 minutes, you will have to log in again to the System.

8. User expired

If you have not logged in to the System in 90 days, your user expires and you need to ask your Administrator to reset it.

9. New User or Password Reset

For a new user who has 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.