Security Statement

FlexBooker users entrust us with their important customer data, and we make it a priority to take their security and privacy concerns seriously. We strive to ensure that user data is kept securely, and that we collect only as much personal data as is required to provide our services to users in an efficient and effective manner.

FlexBooker uses some of the most advanced technology for Internet security that is commercially available today. This Security Statement is aimed at being transparent about our security infrastructure and practices, to help reassure you that your data is appropriately protected.

Application and User Security

- **SSL/TLS Encryption:** FlexBooker data is sent over secured, encrypted SSL/TLS connections. All other communications with the flexbooker.com website are sent over SSL/TLS connections. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) technology (the successor technology to SSL) protect communications by using both server authentication and data encryption. This ensures that user data in transit is safe, secure, and available only to intended recipients.

- **User Authentication:** User data on our database is logically segregated by account-based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on. FlexBooker issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the password of the user.

- **User Passwords:** User application passwords have minimum complexity requirements. Passwords are individually salted and hashed.

- **Data Encryption:** Certain sensitive user data, such as credit card details and account passwords, is stored in encrypted format.

- **Data Portability:** FlexBooker enables you to export your data from our system in a variety of formats so that you can back it up, or use it with other applications.

- **Privacy:** We have a comprehensive privacy policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

- **HIPAA:** We do not explicitly certify HIPAA compliance, but we make every effort to ensure that all data is collected and stored in a manner compliant with HIPAA.

Physical Security

- **Data Centers:** Our information systems infrastructure (servers, networking equipment, etc.) is collocated at third party SSAE 16/SOC 2 audited data centers.

- **Data Center Security:** Our data centers are staffed and surveilled 24/7. Access is secured by security guards, visitors logs, and entry requirements such as passcards and biometric recognition.

- **Environmental Controls:** Our data center is maintained at controlled temperatures and humidity ranges which are continuously monitored for variations. Smoke and fire detection and response systems are in place.

Availability

- **Power:** Servers have redundant internal and external power supplies. Data center has backup power supplies, and is able to draw power from the multiple substations on the grid, several diesel generators, and backup batteries.

- **Uptime:** Continuous uptime monitoring, with immediate escalation to FlexBooker staff for any downtime.

- **Failover:** Our database is log-shipped to standby servers and can failover in less than an hour.

Network Security

- **Uptime:** Continuous uptime monitoring, with immediate escalation to FlexBooker staff for any downtime.
- **Testing:** System functionality and design changes are verified in an isolated test “sandbox” environment and subject to functional and security testing prior to deployment to active production systems.
- **Firewall:** Firewall restricts access to all ports except those required for application functionality.
- **Patching:** Latest security patches are applied to all operating system and application files to mitigate newly discovered vulnerabilities.
- **Access Control:** Secure VPN, multifactor authentication, and role-based access is enforced for systems management by authorized engineering staff.
- **Logging and Auditing:** Central logging systems capture and archive all internal systems access including any failed authentication attempts.

Storage Security

- **Backup Frequency:** Backups occur hourly internally, and daily to a centralized backup system for storage in multiple geographically disparate sites.