bookassist®
technology & online strategy for hotels

Implementacja PCI DSS przez Bookassist
Wersja 2.0

Czym jest PCI DSS

Standardy bezpieczeństwa płatności w Internecie są znane jako PCI DSS (Payment Card Industry Data Security Standards, czyli standardy bezpieczeństwa danych branży kart płatniczych), reprezentujące wymogi Visa i Mastercard dotyczące postępowania z przetwarzaniem kart płatniczych w Internecie. Standardy te pomagają chronić Państwa i Bookassist przed konsekwencjami nieupoważnionego dostępu do kart płatniczych gości.

Mimo że Bookassist dostarcza wszystkie wymagane składniki oprogramowania aby pomóc hotelom w implementacji tych standardów bezpieczeństwa, to hotele używające Systemu Administracyjnego Bookassist są odpowiedzialne za upewnienie się, że ich użytkowanie Systemu spełnia wymogi PCI. Hotele zatem powinny mianować Administratora Systemu Bookassist, który będzie odpowiedzialny za kontrolowanie dostępu pozostałych użytkowników w hotelu.

Proszę zauważyć, że poprzez użytkownie Systemu Administracyjnego Bookassist, zgadzają się Państwo i akceptują Warunki i postanowienia opisane w niniejszym dokumencie.

Warunki i postanowienia

1. Wymogi PCI DSS (standardy ochrony danych osobowych branż kart płatniczych)

Bookassist będzie się właściwie stosować do odpowiednich wymogów Ustawy o Ochronie Danych Osobowych 1988 (zwaną dalej Ustawą), włączając przestrzeganie co następuje: a) zasad o ochronie danych ustanowionych w Ustawie; b) żądań dostępu do danych o podmiotach wysuniętych przez te podmioty; c) wymogów dotyczących rejestracji użytkowników. Jakiekolwiek udostępnienie lub transfer danych przez Bookassist do osób upoważnionych przez podmioty trzecie będzie się odbywać w sposób zgodny z odpowiednimi aktami prawnymi o ochronie danych osobowych. W tym paragrafie “dane” oznaczają wszystkie i jakiekolwiek informacje podane Bookassist lub Dostawcy Zakwaterowania przez osoby trzecie, włączając dane podania, rezerwacji i transakcji związane z danymi płatności kartą kredytową lub inne tego typu dane.
Bokassist dokłada wszelkich starań, aby stosować się do warunków przedstawionych przez standardy bezpieczeństwa danych branży kart płatniczych (PCI DSS) odnośnie przeprowadzania płatności online.

Dostawca Zakwaterowania jest w pełni odpowiedzialny za odpowiednie spełnienie wymogów PCI DSS wdrożonych przez Bookassist odnośnie administrowania lokalnymi użytkownikami mającymi dostęp do Systemu Administracyjnego Bookassist, ochrony nazw użytkownika i haseł do systemu, a w szczególności kontroli nad użytownikami, którym nadano prawa dostępu do danych kart kredytowych gości. W szczególności dostawca zakwaterowania gwarantuje, że:

- będzie stosował się do wymogów bezpieczeństwa PCI DSS;
- uznaje swoją odpowiedzialność za zabezpieczenie danych Posiadacza Karty Kredytowej;
- rozumie, że dane Posiadacza Karty Kredytowej mogą być użyte wyłącznie w celu sfinalizowania transakcji, wspomagania programu lojalnościowego, usługi kontroli nieautoryzowanego dostępu lub w innych celach wymaganych przez prawo;
- będzie współpracował i poda dostęp reprezentatowi firmy kart płatniczych lub autoryzowanej przez tę firmę osobie trzeciej w celu przeprowadzenia pełnego przeglądu bezpieczeństwa po incydencie naruszenia bezpieczeństwa;
- rozumie, że te zobowiązania ochrony prywatności Posiadacza Karty Kredytowej będą obowiązywały również po zakończeniu wszelkich umów z Bookassist.

Jakiekolwiek naruszenie standardów, procedur lub wskazań ustanowionych zgodnie z tą polityką będzie zaprezentowane kierownictwu Dostawcy Zakwaterowania w celu podjęcia odpowiednich działań. Może to zakończyć się działaniem dyscyplinarnym, włączając zwolnienie, zaprzestanie usługi i/lub postępowanie sądowe.

2. Specyfikacje

Poziom dostępu konieczny do wykonania zadania
Dostęp do systemu na określonym poziomie powinien być dany tylko tym użytkownikom, którzy potrzebują tego poziomu dostępu do wykonania swojej pracy.

Dostęp a restrykcje danych
Dostęp powinien być podany tylko po autoryzacji przez kierownika recepcji lub hotelu. Dane karty kredytowej gościa są dostępne w systemie przez miesiąc po dacie wymeldowania gościa. Po tym okresie dane zostają automatycznie usuwane z systemu Bookassist i nie mogą być odzyskane.

Indywidualne dane logowania
Dane logowania muszą być unikalne dla każdego użytkownika. Użytkownicy nie mogą dzielić swoich danych logowania z nikim innym.

Nieaktywni użytkownicy
Dane logowania powinny być usunięte natychmiast jeśli użytkownik już ich nie potrzebuje lub odszedł z pracy.

Nowi użytkownicy
Kiedy dane logowania do Systemu Administracyjnego Bookassist są utworzone dla nowego użytkownika, użytkownik jest zobowiązany przeczytać, zrozumieć i zaakceptować wyżej wymienione warunki.

Uwagi o polityce haseł

Standardy PCI oznaczają, że hasła używane w Systemie Administracyjnym Bookasisst muszą spełniać określone kryteria. Procedury logowania do systemu zapewniają spełnienie wymogów PCI. Weryfikowanie danych logowania przez Bookassist zatwierdza nazwę użytkownika i hasło, a w razie błędów podaje jasny komunikat na ekranie, wyjaśniający co nie jest poprawne i w jaki sposób to naprawić.

Mocne hasła
Wybierz mocne hasło o następujących charakterystykach:

- użyj zarówno małych jak i wielkich liter oraz cyfr i znaków interpunkcyjnych
- nie używaj osobistych informacji lub słów w powszechnym użytku lub do znalezienia w słowniku
- nie dziel hasła z nikim innym
- nie zapisuj hasła i nie zachowuj go w Internecie

Długość ważności hasła
Co 90 dni system wymaga zmiany hasła. Jasne polecenia przeprowadzają użytkownika przez ten proces.

Format hasła
Hasło musi mieć przynajmniej 7 znaków, w tym przynajmniej 1 cyfrę i 1 literę. Jeżeli zmienione hasło nie spełnia tych wymogów, na ekranie pojawia się komunikat wyjaśniający co zrobić aby ustawić ważne hasło.

Historia hasła
Kiedy użytkownik zmienia hasło, System sprawdza czy nie jest ono takie samo jak jedno z czterech ostatnich haseł.

Próby logowania
Kiedy podczas logowania zostanie wpisane niepoprawne hasło, użytkownik ma 6 prób zanim dostęp zostanie odcięty. Jeżeli tak się stanie, użytkownik musi poprosić swojego Administratora aby zresetował hasło i musi odczekać 30 minut zanim będzie mógł się zalogować.

Czas odcięcia dostępu
Jeżeli dostęp zostanie odcięty z powodu wpisania błędnego hasła 6 razy, użytkownik musi odczekać 30 minut zanim będzie mógł się zalogować ponownie, nawet po zresetowaniu hasła przez Administratora.

Wygaśnięcie sesji
PCI wymaga od nas, abyśmy ograniczyli sesję logowania do 15-tu minut braku aktywności. Jeżeli zatem komputer nie jest używany przez 15 minut lub dłużej, użytkownik musi zalogować się ponownie.

Wygaśnięcie hasła
Jeżeli użytkownik nie zaloguje się do Systemu przez 90 dni, hasło wygasa i trzeba poprosić swojego Administratora o zresetowanie hasła.

Nowy użytkownik lub zresetowane hasło
Nowy użytkownik, któremu zostało przesłane tymczasowe hasło lub użytkownik, który poprosił o zresetowanie hasła i któremu zostało przesłane tymczasowe hasło, musi zalogować się tymczasowym hasłem w ciągu 24 godzin od momentu przesłania hasła. Po tym czasie hasło traci ważność i Administrator musi je zresetować.

