Polityka Korzystania z Extranetu Bookassist

Ostatnia aktualizacja: 25 maja 2018 r.

Niniejsza polityka obejmuje:

1. Warunki korzystania z Systemu Administracyjnego Bookassist („System”)

2. Informacje o ochronie danych pracowników / personelu upoważnionego do dostępu do Systemu lub Systemu Zarządzania Treścią Bookassist („CMS”)

3. Informacje wyjaśniające zasady stosowania haseł w Systemie

Należy pamiętać, że korzystając z Systemu Administracyjnego Bookassist („System”), użytkownik potwierdza akceptację Warunków określonych w niniejszym dokumencie. System zapewnia dostęp do danych osobowych na podstawie zobowiązań umownych określonych w Umowie Bookassist z Dostawcą Zakwaterowania oraz zgodnie z Warunkami Przetwarzania i Bezpieczeństwa Danych Bookassist (https://bookassist.org/dp).

1) Warunki korzystania z Systemu Administracyjnego Bookassist („System”)

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

a) Mimo iż Bookassist dokłada wszelkich starań, aby w pełni przestrzegać warunków określonych przez standardy bezpieczeństwa PCI DSS dla przetwarzania płatności kart płatniczych online, Dostawca Zakwaterowania ponosi pełną odpowiedzialność za prawidłowe korzystanie z danych osobowych udostępnionych w Systemie zgodnie z odpowiednimi przepisami o ochronie danych.

b) Dostawca Zakwaterowania musi wyznaczyć Administratora Systemu, który będzie odpowiedzialny za kontrolowanie dostępu innych pracowników lub upoważnionego personelu do Systemu („Użytkownicy”).

c) Dostawca Zakwaterowania ponosi pełną odpowiedzialność za prawidłowe funkcjonowanie wymagań PCI DSS wdrożonych przez Bookassist w zakresie zarządzania Użytkownikami posiadającymi dostęp do Systemu, ochrony nazw użytkowników i haseł do Systemu, a w szczególności kontroli nad Użytkownikami, którym przyznano dostęp do danych karty kredytowej Posiadacza Karty. W szczególności Dostawca Zakwaterowania zapewnia, że:

- będzie przestrzegać wymagań bezpieczeństwa PCI DSS;

- uznaje swoją odpowiedzialność za zabezpieczenie danych Posiadacza Karty;

- uznaje, że dane Posiadacza Karty mogą być wykorzystywane wyłącznie do ułatwienia realizacji transakcji, obsługi programu lojalnościowego, świadczenia usług kontroli oszustw lub do celów wymaganych przez prawo;

- zapewni pełną współpracę i umożliwi przeprowadzenie dokładnego przeglądu bezpieczeństwa przez przedstawiciela branży kart płatniczych lub zatwierdzoną przez branżę kart płatniczych stronę trzecią po naruszeniu bezpieczeństwa;

- uznaje, że te zobowiązania do ochrony poufności danych Posiadacza Karty pozostają w mocy po rozwiązaniu wszelkich innych umów z Bookassist.

d) Każde naruszenie standardów, procedur lub wytycznych ustanowionych zgodnie z niniejszą polityką zostanie przedstawione kierownictwu Dostawcy Zakwaterowania w celu podjęcia odpowiednich działań. Może to skutkować działaniami dyscyplinarnymi, w tym zwolnieniem lub przerwaniem świadczenia usług lub postępowaniem prawnym.

2. Dostęp w koniecznym zakresie

Dostęp do systemu na określonym poziomie powinien być przyznawany tylko tym Użytkownikom, którzy konkretnie potrzebują dostępu na tym poziomie do wykonywania swojej pracy.

3. Ograniczenia dostępu i danych

a) Dostęp powinien być przyznawany wyłącznie za upoważnieniem Dostawcy Zakwaterowania.

b) Dane karty kredytowej Klienta można przeglądać tylko przez maksymalnie 1 (jeden) miesiąc od daty wyjazdu Klienta. Po tym czasie dane są automatycznie usuwane z systemu Bookassist i nie można ich odzyskać.

c) Wszystkie inne Dane Osobowe Klienta są anonimizowane 12 miesięcy po dacie wyjazdu.

4. Indywidualne loginy

Loginy muszą być unikalne dla każdego użytkownika. Użytkownicy nie mogą udostępniać swojego loginu nikomu innemu.

5. Nieaktywni użytkownicy

Loginy powinny być natychmiast usuwane dla Użytkowników, którzy już ich nie potrzebują lub zaprezstali pracy u Dostawy Zakwaterowania.

6. Nowi użytkownicy

Podczas tworzenia loginów do Systemu Użytkownik zobowiązany jest do przeczytania, zrozumienia i zaakceptowania warunków wymienionych powyżej.

2) Informacje o ochronie danych dla pracowników/osób upoważnionych uzyskujących dostęp do Systemu i Systemu lub Systemu Zarządzania Treścią ("CMS")

1. Informacje gromadzone na temat pracowników/upoważnionego personelu ("Użytkowników") uzyskujących dostęp do Systemu lub CMS i dlaczego są one gromadzone i przetwarzane

a) Użytkownicy uzyskujący dostęp do Systemu lub CMS są zobowiązani do podania imienia i nazwiska, adresu e-mail, telefonu. Ponadto System i CMS rejestrują logi wszystkich dostępów i działań.

b) Tego rodzaju gromadzenie i przetwarzanie danych jest niezbędne do zapewnienia funkcjonalności Systemu i CMS oraz do analizowania problemów w celu umożliwienia nam reagowania na nie.

2. W jaki sposób dane użytkownika mogą być wykorzystywane i kto ma do nich dostęp?

Dane użytkownika służą do obsługi funkcjonowania systemu i CMS. Dostawca Zakwaterowania Zakwaterowania może zażądać dostępu do danych użytkownika. W celu uzyskania szczegółowych informacji na temat sposobu wykorzystania tych danych, należy skontaktować się z odpowiednim Dostawcą Zakwaterowania. Należy pamiętać, że jeśli Dostawca Zakwaterowania zażądał danych użytkownika, może zachować do nich dostęp przez inny okres przechowywania.

3. Prawa Użytkownika

Użytkownicy mają prawo dostępu do swoich danych, ich sprostowania i usunięcia, a także prawo do przenoszenia danych oraz prawo do wniesienia skargi do właściwego organu nadzorczego zgodnie z odpowiednimi wymogami ochrony danych.

4. Przechowywanie

Wszystkie dane wymienione w punkcie 1 będą przechowywane przez Bookassist przez okres dwóch lat od daty wygaśnięcia konta użytkownika.

5. Kontakt

Użytkownik może wysłać wiadomość e-mail do osoby kontaktowej ds. ochrony danych Bookassist na adres dpo@bookassist.com, jeśli potrzebuje dalszych informacji lub chciałby skorzystać z przysługujących mu praw

3) Wyjaśnienia dotyczące polityki haseł w zakresie korzystania z Systemu

Standardy PCI oznaczają, że hasła używane w Systemie muszą spełniać określony zestaw zasad. Procedura logowania w Systemie zapewnia, że standardy PCI są spełnione. W procesie kontroli logowania, Bookassist zweryfikuje nazwę użytkownika i hasło, a w przypadku błędów wyświetli na ekranie jasne komunikaty wyjaśniające, co jest nieprawidłowe i jak je poprawić.

1. Silne hasła

Należy wybierać silne hasła o następujących cechach:

- używaj zarówno wielkich, jak i małych liter, a także cyfr lub znaków interpunkcyjnych
- nie używaj danych osobowych ani słów powszechnie używanych lub znalezionych w słowniku
- nie udostępniaj nikomu hasła
- nie zapisuj hasła ani nie przechowuj go online.

2. Wiek hasła

System wymaga zmiany hasła co 90 dni. Przejrzyste instrukcje przeprowadzą użytkownika przez ten proces.

3. Format hasła

Długość hasła musi wynosić co najmniej 7 znaków, w tym co najmniej 1 cyfrę i 1 znak alfabetu. W przypadku zmiany hasła, które nie spełnia tych wymagań, na ekranie zostanie wyświetlony komunikat z informacją, co należy zrobić, aby hasło było prawidłowe.

4. Historia haseł

Po zmianie hasła system sprawdza, czy nie jest ono tożsame z żadnym z 4 ostatnich haseł.

5. Próby logowania

Jeśli podczas logowania wprowadzisz nieprawidłowe hasło, masz łącznie 6 prób, zanim zostaniesz zablokowany. W takim przypadku należy poprosić administratora o zresetowanie hasła i odczekać 30 minut, aby ponownie się zalogować.

6. Czas blokady

Jeśli użytkownik został zablokowany w Systemie z powodu 6-krotnego wprowadzenia nieprawidłowego hasła, musi odczekać 30 minut przed ponownym zalogowaniem, nawet po zresetowaniu hasła przez administratora.

7. Limit czasu sesji

PCI wymaga od nas ograniczenia sesji logowania do 15 minut bezczynności. Jeśli komputer był bezczynny przez dłużej niż 15 minut, konieczne będzie ponowne zalogowanie się do systemu.

8. Wygaśnięcie konta Użytkownika

W sytuacji gdy Użytkownik nie logował się do Systemu przez 90 dni, jego konto wygasa i należy zwrócić się do administratora o jego zresetowanie.

9. Nowy użytkownik lub reset hasła

W przypadku nowego Użytkownika, któremu wysłano hasło tymczasowe, lub Użytkownika, który zwrócił się o reset hasła i otrzymał nowe hasło, Użytkownik musi zalogować się przy użyciu hasła tymczasowego w ciągu 24 godzin. Po tym czasie hasło wygasa, a administrator musi je zresetować.