

Wytyczne bezpieczeństwa dot. przetwarzania danych płatniczych

- *Niniejszy dokument zawiera zespół obowiązków Partnera w związku z korzystaniem z usług świadczonych przez PayU z wykorzystaniem Tokenu.*
- *Pojęciom napisanym z wielkiej litery a nie zdefiniowanym w tym dokumencie nadaje się znaczenie jak w Regulaminie Systemu, Regulaminie Usługi Płatności Kartami Płatniczymi, Regulamin usługi płatności elektronicznych oraz Umowie na udostępnienie usługi.*

W celu podniesienia poziomu bezpieczeństwa płatności internetowych, każdy Partner przetwarzający, przechowujący lub przesyłający dane płatnicze, powinien wdrożyć odpowiednie mechanizmy bezpieczeństwa w systemach IT. Przez dane płatnicze, rozumiemy wszystkie narzędzia za pomocą których można dokonywać płatności internetowych, w skład których wchodzi również Tokeny reprezentujące instrumenty płatnicze (np. karty). Przy czym na żądanie PayU Partnerzy powinni wyjaśnić i uzasadnić wszelkie przypadki braku zgodności stosowanej w ich działalności praktyki.

Poniżej przedstawiamy mechanizmy bezpieczeństwa jakie powinien wdrożyć Partner:

1 Zarządzanie uprawnieniami dostępu do systemów IT:

- Dostęp do systemów IT (serwer, firewall, urządzenie sieciowe, środowiska testowe i produkcyjne, itp) powinien wynikać z pełnionych przez pracownika obowiązków oraz spełniać zasadę nadawania minimalnych potrzebnych uprawnień
- odpowiedniego podziału zadań w środowiskach informatycznych (np. środowiskach rozwojowych, testowych i produkcyjnych)
- Każdy użytkownik powinien posiadać swój indywidualny login i hasło dostępowe spełniające odpowiedni poziom bezpieczeństwa (rekomendowane ustawienia to długość hasła minimum 8 znaków, wykorzystanie 3 z parametrów: wielka litera, mała litera, cyfra, znak specjalny)

2. Bezpieczeństwo sieci i systemów:

- Przesyłanie wrażliwych danych płatniczych przez sieć publiczną powinno być zabezpieczone z wykorzystaniem bezpiecznych metod transmisji, takich jak TLS (rekomendowane protokoły to TLS 11 lub wyższe)
- Systemy IT powinny być skonfigurowane zgodnie z dobrymi praktykami bezpieczeństwa, takimi jak NIST, SANS, itp.

3. Monitoring , testy bezpieczeństwa i audyty

- Dostęp do krytycznych zasobów IT (sieci, bazy danych, itp.) powinien być monitorowany oraz śledzony.
- Systemy IT powinny podlegać okresowym testom bezpieczeństwa oraz audytom pod kątem wykrywania zagrożeń, luk i podatności. Audyty powinny być przeprowadzane przez niezależnych ekspertów.