Wytyczne bezpieczeństwa dla Sprzedawców dotyczące przetwarzania danych płatniczych

- **Niniejszy dokument zawiera wytyczne bezpieczeństwa dla Sprzedawcy w związku z korzystaniem z usług świadczonych przez Polskie ePłatności Sp. z o.o. z wykorzystaniem Tokenu.**
- **Wytyczne są uzupełnieniem Regulaminu świadczenia usług Polskich ePłatności dostępnym TUTAJ**

Sprzedawca powinien po swojej stronie wdrożyć co najmniej następujące mechanizmy bezpieczeństwa:

1. Zarządzanie uprawnieniami dostępu do systemów IT:

a. 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.

b. odpowiedniego podziału zadań w środowiskach informatycznych (np. środowiskach rozwojowych, testowych i produkcyjnych).

c. 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:

a. Przesyłanie wrażliwych danych płatniczych przez sieć publiczną powinno być zabezpieczone z wykorzystaniem bezpiecznych metod transmisji, takich jak TLS (rekomendowane protokoły to TLS 1.3 lub wyższe, minimalny dopuszczalny 1.2).

b. Systemy IT powinny być skonfigurowane zgodnie z dobrymi praktykami bezpieczeństwa, takimi jak NIST, SANS, itp.

3. Monitoring, testy bezpieczeństwa i audyty:

a. Dostęp do krytycznych zasobów IT (sieci, bazy danych, itp.) powinien być monitorowany oraz śledzony.

b. Systemy IT powinny podlegać okresowym testom bezpieczeństwa oraz audytom pod kątem wykrywania zagrożeń, luk i podatności. Audyty powinny być przeprowadzane przez niezależnych ekspertów.