

Poniższa lista ostrzeżeń dotyczących bezpieczeństwa użytkowania produktu oparta jest o wymagania Rozporządzenia (UE) 2023/988 (GPSR). Naszym celem jest ochrona użytkowników przed potencjalnymi zagrożeniami wynikającymi z nieodpowiedniego użytkowania. Informacje przedstawione są w prosty sposób by były zrozumiałe i przejrzyste dla wszystkich użytkowników, w tym również dla osób starszych oraz osób z ograniczeniami ruchowymi.

## **Instrukcja bezpieczeństwa użytkowania produktu UniFi Express (UX) - router bezprzewodowy Cloud Gateway**

### **1. Bezpieczeństwo instalacji i montażu**

- Urządzenia należy montować w suchych pomieszczeniach, z dala od źródeł wilgoci i bezpośredniego działania wody.
- Urządzenia powinny być umieszczone na stabilnej powierzchni lub zamocowane zgodnie z instrukcją producenta, aby zapobiec upadkowi i uszkodzeniom mechanicznym.
- Unikać instalacji w miejscach narażonych na silne wstrząsy lub drgania, które mogą uszkodzić urządzenie lub wpłynąć na jego działanie.
- Nie blokować otworów wentylacyjnych urządzenia, aby zapewnić odpowiednią cyrkulację powietrza i zapobiec przegrzewaniu.

### **2. Bezpieczeństwo elektryczne i zasilania**

- Podłączenie urządzenia do sieci elektrycznej powinno być wykonane zgodnie z zaleceniami producenta i obowiązującymi normami.
- Używać wyłącznie oryginalnych lub zalecanych zasilaczy i kabli zasilających.
- Nie używać uszkodzonych przewodów zasilających ani portów sieciowych.
- Unikać przeciążania gniazd zasilających i sieciowych, co może prowadzić do przegrzania lub uszkodzenia urządzenia.
- Nie ciągnąć za przewód zasilający podczas odłączania urządzenia – zawsze chwytać za wtyczkę.

### **3. Bezpieczeństwo użytkowania**

- Nie używać urządzenia, jeśli jest uszkodzone lub wykazuje nieprawidłowe działanie, np. niestabilne połączenie, przegrzewanie, nietypowe dźwięki.
- Nie modyfikować ani nie demontować urządzenia samodzielnie – wszelkie naprawy powinny być wykonywane przez autoryzowany serwis.

### **4. Bezpieczeństwo dzieci**

- Urządzenia nie są zabawkami i powinny być przechowywane poza zasięgiem dzieci.
- Małe elementy, takie jak śruby montażowe czy zaślepki, mogą stanowić ryzyko zadławienia – należy je przechowywać w bezpiecznym miejscu.

### **5. Zagrożenia cyberbezpieczeństwa**

- Urządzenie musi być zabezpieczone przed nieautoryzowanym dostępem. Używaj tylko silnych haseł.
- Regularna zmiana hasła jest podstawowym elementem odpowiedniego zabezpieczenia systemu.
- Należy stosować ograniczenia uprawnień użytkowników urządzenia. Każdy użytkownik powinien mieć tylko niezbędne uprawnienia.

- Jeżeli to możliwe wykonuj segmentację sieci za pośrednictwem VLAN. Odpowiednio podzielona sieć pozwala na odseparowanie ruchu pomiędzy poszczególnymi grupami urządzeń.
- Unikaj bezpośredniego wystawiania urządzenia do sieci publicznej poprzez przekierowanie portów. Do dostępu zdalnego korzystaj z funkcji chmurowych, jeżeli urządzenie je posiada lub z połączeń VPN.
- Jeżeli urządzenie posiada panel WEB, korzystaj z szyfrowanych połączeń HTTPS.
- Należy regularnie przeprowadzać aktualizację oprogramowania urządzenia aby zapewnić ochronę przed nowymi zagrożeniami.
- Należy zapewnić wszystkie możliwe środki ochrony sieci i danych osobowych.
- Wyłącz funkcje sieciowe i protokoły jak UPnP, jeżeli nie są potrzebne we wdrażanym systemie.
- Regularnie wykonuj audyty bezpieczeństwa, co pewien czas należy przeprowadzać testy bezpieczeństwa i aktualizować polityki ochrony.

## **6. Prawidłowe usuwanie zużytego urządzenia**

- Produkt należy utylizować zgodnie z miejscowymi przepisami dotyczącymi gospodarki odpadami elektronicznymi i niebezpiecznymi.

## **7. Znaczenie stosowania się do ostrzeżeń**

- Zastosowanie się do przedstawionych tu ostrzeżeń minimalizuje ryzyko uszkodzeń ciała, awarii urządzenia oraz strat materialnych wynikających z nieumiejętnego obchodzenia się produktem.