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 OC300 - kontroler sprzętowy Omada (do 500 punktów dostępowych)

1. **Ogólne zasady bezpieczeństwa**
   - Przed obsługą urządzenia należy zapoznać się z instrukcją obsługi produktu dostarczoną przez producenta i informacjami dotyczącymi bezpieczeństwa w niej zawartymi.
   - Używaj produkt zgodnie z jego przeznaczeniem określonym w instrukcji obsługi.
   - To urządzenie może być używane wyłącznie przez osoby o wystarczającej sprawności fizycznej, sensorycznej i intelektualnej oraz posiadającej odpowiednią wiedzę i doświadczenie. Inne osoby mogą korzystać z urządzenia wyłącznie pod nadzorem osób odpowiedzialnych za ich bezpieczeństwo.
   - Trzymaj ten produkt z dala od dzieci. Dzieci nie są jeszcze w stanie ocenić istniejących zagrożeń.
   - Przechowywać elementy opakowania (woreczki foliowe, elementy ze styropianu) poza zasięgiem dzieci i zwierząt.
2. **Bezpieczeństwo instalacji i montażu**
   - Kontrolery sprzętowe należy instalować w suchych, wentylowanych pomieszczeniach, z dala od źródeł wilgoci i skrajnych temperatur.
   - Urządzenia montować na stabilnych powierzchniach lub w szafach rack zgodnie z zaleceniami producenta, zapewniając odpowiednią wentylację i dostęp do portów.
   - Unikać instalacji w miejscach narażonych na wstrząsy lub drgania, które mogą uszkodzić podzespoły elektroniczne.
   - Nie blokować otworów wentylacyjnych, aby zapobiec przegrzewaniu się urządzenia.
3. **Bezpieczeństwo elektryczne i zasilania**
   - Podłączenie urządzenia do sieci elektrycznej powinno być wykonane zgodnie z obowiązującymi normami i najlepiej przez wykwalifikowany personel.
   - Sprawdzać zgodność napięcia zasilania z wymaganiami urządzenia oraz stan przewodów zasilających.
   - Nie używać uszkodzonych kabli zasilających ani nie ciągnąć za przewody podczas odłączania urządzenia.
   - W przypadku zasilania PoE stosować odpowiednie zabezpieczenia i upewnić się, że urządzenie jest kompatybilne z dostarczanym napięciem.
   - Unikać przeciążania gniazd zasilających i stosować zabezpieczenia przeciwprzepięciowe.
4. **Bezpieczeństwo użytkowania**
   - Nie używać urządzenia, jeśli jest uszkodzone lub wykazuje nieprawidłowe działanie, np. przegrzewanie, nieprawidłowe sygnalizacje lub brak łączności.

- Nie demontować ani nie modyfikować urządzenia; wszelkie naprawy powinny być wykonywane wyłącznie przez autoryzowany serwis.
- Unikać kontaktu urządzenia z cieczami oraz nie obsługiwać urządzenia mokrymi rękami.
- Przed czyszczeniem odłączyć urządzenie od zasilania i używać miękkiej, suchej ściereczki bez środków chemicznych.

5. **Bezpieczeństwo środowiskowe**
   - Przechowywać i eksploatować urządzenie w temperaturach zgodnych z danymi producenta.
   - Unikać ekspozycji na bezpośrednie światło słoneczne oraz skrajne warunki atmosferyczne.
   - Utrzymywać wilgotność względną w zakresie zalecanym przez producenta.

6. **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.

7. **Prawidłowe usuwanie zużytego urządzenia**
   - Produkt należy utylizować zgodnie z miejscowymi przepisami dotyczącymi gospodarki odpadami elektronicznymi i niebezpiecznymi.

8. **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.

Na każdym etapie użytkowania urządzenia należy przestrzegać zasad i informacji bezpieczeństwa zawartych w instrukcji obsługi produktu dostarczonej przez producenta. Zachowaj instrukcję obsługi abyś mógł się w każdej chwili do niej odnieść. Urządzenie należy przekazywać osobom trzecim wyłącznie wraz z instrukcją użytkowania.