

*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 MC16-PAC-EX - Kontroler dostępu w wersji EX**

### **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 montażu i instalacji**

- Instalacja urządzenia powinna być wykonana zgodnie z instrukcją producenta, przez wykwalifikowanego instalatora z odpowiednią wiedzą techniczną.
- Kontrolery dostępu należy instalować wyłącznie w suchych, wentylowanych pomieszczeniach, z dala od źródeł wilgoci i skrajnych temperatur.
- Montaż urządzenia powinien być wykonany stabilnie, z użyciem odpowiednich elementów mocujących dostarczonych przez producenta.
- Podczas instalacji należy unikać uszkodzenia przewodów oraz elementów elektronicznych kontrolera.
- Nie wolno modyfikować ani demontować urządzenia; wszelkie naprawy powinny być wykonywane przez wykwalifikowany serwis.

### **3. Bezpieczeństwo elektryczne i zasilanie**

- Podłączenie zasilania należy wykonać zgodnie z wymaganiami producenta, stosując odpowiednie napięcie oraz zabezpieczenia przeciwprzepięciowe.
- Nie wolno używać uszkodzonych przewodów zasilających ani interfejsowych.
- Podczas podłączania interfejsów należy zachować ostrożność, aby uniknąć zwarcia i uszkodzeń urządzenia.
- Ładowanie i monitorowanie baterii rezerwowej powinno odbywać się zgodnie z instrukcją producenta, aby zapewnić ciągłość działania systemu.

### **4. Bezpieczeństwo użytkowania**

- Urządzenie należy użytkować zgodnie z przeznaczeniem i instrukcją obsługi dostarczoną przez producenta.

- Nie dopuszczać do kontaktu urządzenia z wilgocią lub cieczami, które mogą spowodować uszkodzenia lub zagrożenie porażeniem prądem.
- W przypadku wykrycia uszkodzenia lub nieprawidłowego działania należy niezwłocznie odłączyć urządzenie od zasilania i skontaktować się z serwisem.

## **5. Bezpieczeństwo dzieci**

- Kontrolery dostępu nie są zabawkami i powinny być przechowywane z dala od dzieci.
- Małe elementy, takie jak śruby, złącza czy karty pamięci, mogą stanowić ryzyko zadławienia i powinny być przechowywane poza zasięgiem dzieci.

## **6. Konserwacja i serwis**

- Wszelkie prace serwisowe i konserwacyjne powinny być wykonywane przez wykwalifikowany personel zgodnie z zaleceniami producenta.
- Nie należy samodzielnie modyfikować oprogramowania ani sprzętu kontrolera, aby nie naruszyć integralności systemu i bezpieczeństwa danych.
- Regularnie sprawdzaj poprawność działania systemu oraz stan baterii rezerwowej.

## **7. 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.

## **8. Prawidłowe usuwanie zużytego urządzenia**

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

## **9. 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.*