

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 VTO4201F-P1 - moduł stacji bramowej IP**

### **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**

- Moduły główne z kamerą należy instalować zgodnie z instrukcjami producenta, zapewniając stabilne i trwałe mocowanie w wyznaczonym miejscu.
- Przed montażem sprawdź, czy miejsce instalacji jest suche i zabezpieczone przed bezpośrednim działaniem wilgoci oraz ekstremalnych temperatur.
- Unikaj instalacji modułu w miejscach narażonych na wstrząsy lub uderzenia mechaniczne, które mogą uszkodzić kamerę lub elektronikę.
- Podczas montażu zachowaj ostrożność, aby nie uszkodzić przewodów i złączy, szczególnie interfejsów RJ45 oraz 2-Wire.
- Używaj wyłącznie oryginalnych lub zalecanych akcesoriów montażowych i przewodów.

### **3. Bezpieczeństwo zasilania i połączeń sieciowych**

- Podłączaj moduł wyłącznie do zasilania o parametrach zgodnych z zaleceniami producenta.
- Wykonuj połączenia sieciowe (RJ45 Ethernet 10/100Mbps) zgodnie z obowiązującymi normami i zasadami bezpieczeństwa elektrycznego.
- Nie uszkadzaj przewodów i złączy podczas instalacji i eksploatacji; uszkodzone przewody stanowią zagrożenie porażenia prądem oraz mogą powodować nieprawidłową pracę urządzenia.
- Unikaj przeciążania obwodów przekaźnikowych i alarmowych; stosuj zabezpieczenia zgodne z instrukcją.
- W przypadku stosowania interfejsu RS485 do sterowania urządzeniami zewnętrznymi, zapewnij prawidłowe połączenia i izolację, aby uniknąć zakłóceń i uszkodzeń.

### **4. Bezpieczeństwo użytkowania**

- Nie używaj urządzenia, jeśli zauważysz uszkodzenia mechaniczne, nieprawidłowe działanie kamery lub inne nieprawidłowości.
- Nie demontuj ani nie modyfikuj modułu; wszelkie naprawy powinny być wykonywane przez wykwalifikowany serwis.
- Unikaj kontaktu modułu z cieczami; w przypadku zalania natychmiast odłącz zasilanie i skontaktuj się z serwisem.
- Podczas czyszczenia używaj miękkiej, suchej ściereczki; nie stosuj środków chemicznych ani rozpuszczalników.
- Nie używaj urządzenia pod wpływem alkoholu lub środków odurzających.

## **5. Bezpieczeństwo dzieci**

- Moduły nie są zabawkami i powinny być przechowywane poza zasięgiem dzieci.
- Małe elementy montażowe i opakowania mogą stanowić ryzyko zadławienia – należy je odpowiednio zabezpieczyć i usunąć po instalacji.

## **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.

*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.*