

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 ART-ARC3000H-03-GW2(868) - zestaw alarmowy KIT (WiFi, 2G)

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

- Instalację systemu alarmowego wykonuj zgodnie z instrukcją producenta i obowiązującymi przepisami prawa.
- Upewnij się, że centrala alarmowa oraz czujniki są zamontowane w miejscach suchych, chronionych przed wilgocią i bezpośrednim działaniem promieni słonecznych.
- Unikaj montażu czujników w miejscach narażonych na silne wstrząsy lub drgania, które mogą powodować fałszywe alarmy.
- Zachowaj odpowiednią odległość między centralą a czujnikami, aby zapewnić stabilną łączność bezprzewodową.
- Podczas montażu stosuj wyłącznie oryginalne elementy mocujące dołączone do zestawu.

3. Bezpieczeństwo zasilania i sieci

- Podłącz centralę alarmową do zasilania zgodnie z zaleceniami producenta, korzystając z oryginalnego zasilacza.
- Zapewnij stabilne i bezpieczne źródło zasilania, unikając przeciążeń i uszkodzeń przewodów.
- W przypadku systemów z łącznością WiFi, 2G lub LTE, zabezpiecz sieć przed nieautoryzowanym dostępem, stosując silne hasła i aktualizując oprogramowanie.
- Nie używaj uszkodzonych kabli ani zasilaczy, aby uniknąć ryzyka porażenia prądem lub uszkodzenia urządzenia.

4. Bezpieczeństwo użytkowania

- Nie demontuj ani nie modyfikuj elementów systemu alarmowego; wszelkie naprawy wykonuj wyłącznie przez autoryzowany serwis.

- Regularnie sprawdzaj stan baterii w czujnikach i pilocie, aby zapewnić ciągłość działania systemu.
- Nie używaj systemu pod wpływem alkoholu lub środków odurzających, aby uniknąć błędnej obsługi.
- W przypadku wykrycia uszkodzenia lub nieprawidłowego działania systemu, niezwłocznie skontaktuj się z serwisem.
- Nie blokuj ani nie zasłaniaj czujników ruchu i magnetycznych, aby zapewnić ich prawidłowe działanie.

5. Bezpieczeństwo dzieci

- Trzymaj piloty i inne elementy systemu z dala od dzieci, aby uniknąć przypadkowego uruchomienia alarmu lub uszkodzenia urządzeń.
- Małe elementy i baterie mogą stanowić ryzyko zadławienia, dlatego nie pozostawiaj ich w zasięgu dzieci.

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.