

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 ARC3000H-GW2(868) - bezprzewodowa centrala alarmowa (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 centrali alarmowej powinien przeprowadzać wykwalifikowany specjalista, aby zapewnić prawidłowe działanie i bezpieczeństwo systemu.
- Wybierz miejsce montażu chronione przed wilgocią, bez bezpośredniego narażenia na wodę lub skraplanie się pary wodnej.
- Unikaj instalacji w miejscach o wysokiej temperaturze lub narażonych na bezpośrednie działanie promieni słonecznych, co może wpłynąć na żywotność urządzenia.
- Zachowaj odpowiednią wentylację wokół centrali, aby zapobiec przegrzewaniu się urządzenia.
- Podczas montażu zwróć uwagę na stabilność mocowania, aby zapobiec uszkodzeniom mechanicznym lub przypadkowemu odłączeniu.

3. Bezpieczeństwo elektryczne i zasilanie

- Podłączanie centrali do sieci elektrycznej powinno odbywać się zgodnie z obowiązującymi normami i przepisami, najlepiej przez wykwalifikowanego elektryka.
- Upewnij się, że napięcie zasilania jest zgodne z wymaganiami producenta.
- Nie używaj uszkodzonych przewodów zasilających ani wtyczek.
- Unikaj przeciążania gniazd zasilających, do których podłączona jest centrala.
- W przypadku awarii zasilania korzystaj z zasilania awaryjnego (np. baterii wbudowanych w centralę), aby zapewnić ciągłość działania systemu.

4. Bezpieczeństwo komunikacji i konfiguracji

- Używaj wyłącznie oficjalnego oprogramowania i aplikacji producenta (np. DMSS) do konfiguracji i obsługi centrali.

- Zabezpiecz dostęp do aplikacji i centrali silnym hasłem, aby zapobiec nieautoryzowanemu dostępowi.
- Regularnie aktualizuj oprogramowanie centrali, aby zapewnić ochronę przed znanymi zagrożeniami.
- Wykorzystuj szyfrowanie AES128 do zabezpieczenia komunikacji bezprzewodowej i unikaj zakłóceń sygnału.
- Ustaw strefy alarmowe zgodnie z zaleceniami producenta i specyfiką chronionego obiektu.

5. Bezpieczeństwo użytkownika i dzieci

- Nie pozwalaj dzieciom na samodzielną obsługę centrali alarmowej ani urządzeń peryferyjnych.
- Przechowuj piloty i inne akcesoria zdalnego sterowania poza zasięgiem dzieci, aby uniknąć przypadkowego uruchomienia alarmu.
- Nie używaj centrali pod wpływem alkoholu lub środków odurzających, aby zapewnić prawidłową reakcję w sytuacjach alarmowych.

6. Konserwacja i serwis

- Regularnie sprawdzaj stan baterii i wymieniaj je zgodnie z zaleceniami producenta, aby zapewnić ciągłość działania systemu.
- Nie dokonuj samodzielnych napraw ani modyfikacji urządzenia; wszelkie prace serwisowe powinny być wykonywane przez autoryzowany serwis.
- W przypadku wykrycia uszkodzeń lub nieprawidłowego działania natychmiast odłącz urządzenie od zasilania i skontaktuj się z serwisem.

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.