

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 DS-KIS613-S - zestaw wideodomofonowy 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

- Wideodomofony IP należy montować zgodnie z instrukcjami producenta, używając wyłącznie oryginalnych elementów montażowych.
- Panel zewnętrzny powinien być instalowany na stabilnej, odpornej na warunki atmosferyczne powierzchni, na wysokości zapewniającej prawidłowe działanie kamery i mikrofonu.
- Podczas montażu należy unikać uszkodzenia przewodów sieciowych i zasilających, które mogą powodować awarie lub zagrożenie porażeniem prądem.
- Nie należy modyfikować ani demontować urządzeń; wszelkie naprawy powinny być wykonywane przez wykwalifikowany personel.

3. Bezpieczeństwo zasilania i elektryczne

- Podłączanie zasilania należy wykonywać zgodnie z wymaganiami technicznymi zestawu, najlepiej przez wykwalifikowanego elektryka.
- W przypadku stosowania zasilaczy wtorkowych należy upewnić się, że napięcie i natężenie są zgodne z parametrami urządzenia.
- Unikać przeciążania gniazd zasilających oraz stosować odpowiednie zabezpieczenia przeciwprzepięciowe.
- Nie dotykać przewodów i wtyczek mokrymi rękami oraz nie używać urządzenia w warunkach podwyższonej wilgotności bez odpowiedniej ochrony.

4. Bezpieczeństwo użytkowania

- Nie używać uszkodzonych urządzeń – w przypadku zauważenia uszkodzeń należy natychmiast odłączyć sprzęt i skontaktować się z serwisem.

- Nie modyfikować ani nie demontować urządzeń samodzielnie.
- Nie używać wideodomofonu pod wpływem alkoholu lub środków odurzających.
- Zapewnić odpowiednią wentylację monitorów i innych elementów systemu, nie zasłaniać otworów wentylacyjnych.
- Chronić urządzenia przed wilgocią i ekstremalnymi temperaturami, które mogą wpłynąć na ich działanie.

5. Bezpieczeństwo sieci i danych

- Podłączanie urządzeń do sieci IP powinno odbywać się z zachowaniem zasad bezpieczeństwa sieciowego, stosując silne hasła i aktualizacje oprogramowania.
- Regularnie aktualizować oprogramowanie urządzeń, aby zapewnić ochronę przed zagrożeniami cybernetycznymi.
- Unikać podłączania urządzeń do niezabezpieczonych sieci publicznych.

6. Bezpieczeństwo dzieci

- Wideodomofony nie są zabawkami – trzymać z dala od dzieci, aby zapobiec przypadkowemu uszkodzeniu lub zadławieniu małymi elementami.
- Małe elementy i opakowania mogą stanowić ryzyko zadławienia, należy je odpowiednio zabezpieczyć i usunąć z zasięgu dzieci.

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.