

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 SCP3022B-IBZ - panel sterowania do wideodomofonu

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 instalacji i montażu

- Monitory należy montować zgodnie z instrukcją producenta, zapewniając stabilne i bezpieczne mocowanie na ścianie lub w dedykowanym miejscu.
- Podczas instalacji korzystaj z oryginalnych akcesoriów i przewodów 2-żyłowych dostarczonych lub rekomendowanych przez producenta.
- Unikaj uszkodzenia przewodów podczas montażu, nie zgniataj ani nie przecinaj kabli.
- Zapewnij odpowiednią wentylację wokół urządzenia, nie zasłaniaj otworów wentylacyjnych monitora.
- Nie instaluj monitora w miejscach narażonych na bezpośrednie działanie wilgoci lub wody.

3. Bezpieczeństwo elektryczne i zasilanie

- Podłączanie monitora do zasilania i sieci powinno być wykonane zgodnie z wymaganiami producenta oraz przez wykwalifikowany personel.
- Używaj tylko przewodów i złączy zgodnych z normami oraz dedykowanych do systemów 2-wire IP Dahua.
- Nie uszkadzaj przewodów zasilających i komunikacyjnych, unikaj ciągnięcia za przewód podczas podłączania lub odłączania.
- Przed podłączeniem sprawdź zgodność napięcia zasilania z wymaganiami monitora.
- W przypadku uszkodzenia przewodów lub urządzenia nie używaj go i skontaktuj się z serwisem.

4. Bezpieczeństwo użytkowania

- Nie używaj monitora pod wpływem alkoholu lub środków odurzających.
- Unikaj kontaktu urządzenia z wilgocią, jeśli nie jest do tego przystosowane.

- Nie demontuj ani nie modyfikuj urządzenia samodzielnie; wszelkie naprawy powinny być wykonywane przez specjalistów.
- Nie zasłaniaj ekranu monitora oraz nie narażaj go na silne uderzenia mechaniczne.
- W przypadku zauważenia nieprawidłowości w działaniu urządzenia, wyłącz je i skontaktuj się z serwisem.

5. Bezpieczeństwo dzieci

- Monitory nie są zabawkami i powinny być trzymane poza zasięgiem małych dzieci.
- Elementy montażowe i opakowania mogą stanowić ryzyko zadławienia, dlatego należy je przechowywać z dala od dzieci.

6. Bezpieczeństwo sieci i komunikacji

- Konfigurację sieciową i dostęp do monitorów należy zabezpieczyć silnymi hasłami i aktualizować oprogramowanie zgodnie z zaleceniami producenta.
- Unikaj podłączania urządzenia do niezabezpieczonych sieci Wi-Fi, aby zapobiec nieautoryzowanemu dostępowi.
- W przypadku korzystania z funkcji interkomu i zdalnego sterowania, stosuj środki ochrony prywatności i bezpieczeństwa danych.

7. Konserwacja i czyszczenie

- Przed czyszczeniem monitora odłącz go od zasilania.
- Do czyszczenia używaj miękkiej, suchej lub lekko wilgotnej szmatki. Nie stosuj środków chemicznych, które mogą uszkodzić ekran lub obudowę.
- Regularnie sprawdzaj stan przewodów i złączy pod kątem uszkodzeń.

8. 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.

9. Prawidłowe usuwanie zużytego urządzenia

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

10. 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.