

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 SCP3022A-B - 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 montażu i instalacji

- Monitor IP Dahua należy montować w suchych pomieszczeniach, z dala od źródeł wilgoci i bezpośredniego działania wody.
- Urządzenie powinno być stabilnie zamocowane na ścianie lub innym podłożu, zgodnie z instrukcją producenta, aby zapobiec upadkowi i uszkodzeniom mechanicznym.
- Podczas instalacji należy unikać uszkodzenia przewodów komunikacyjnych i zasilających, szczególnie przewodu Ethernet oraz przewodu 2-Wire, jeśli jest stosowany.
- Podłączenie elektryczne i sieciowe powinno być wykonane zgodnie z obowiązującymi normami i najlepiej przez wykwalifikowany personel.
- Nie należy modyfikować ani demontować urządzenia samodzielnie; wszelkie naprawy powinny być wykonywane przez autoryzowany serwis.

3. Bezpieczeństwo zasilania i sieci

- Monitor należy zasilac zgodnie z wymaganiami producenta, używając odpowiedniego źródła zasilania i zabezpieczeń przeciwprzepięciowych.
- Przewody zasilające i sieciowe powinny być sprawdzane pod kątem uszkodzeń przed instalacją i regularnie podczas użytkowania.
- Nie ciągnąć ani nie zginać przewodów w sposób mogący je uszkodzić.
- W przypadku wykrycia uszkodzeń przewodów należy natychmiast odłączyć urządzenie i skontaktować się z serwisem.
- Monitor wyposażony jest w moduł Wi-Fi 2,4 GHz – należy zapewnić odpowiednie zabezpieczenia sieci bezprzewodowej, aby zapobiec nieautoryzowanemu dostępowi.

4. Bezpieczeństwo użytkowania

- Nie używać urządzenia, jeśli obudowa jest uszkodzona lub jeśli urządzenie wykazuje nieprawidłowe działanie, takie jak zakłócenia obrazu, dźwięku lub brak reakcji na dotyk.
- Nie dotykać monitora mokrymi rękami, aby uniknąć ryzyka porażenia prądem.
- Nie zasłaniać otworów wentylacyjnych monitora, aby zapobiec przegrzaniu.
- Podczas czyszczenia monitora wyłączyć urządzenie z zasilania i używać miękkiej, suchej ściereczki; unikać stosowania środków chemicznych mogących uszkodzić ekran lub obudowę.
- Nie używać monitora pod wpływem alkoholu lub środków odurzających.

5. Bezpieczeństwo dzieci

- Monitory IP Dahua nie są zabawkami i powinny być przechowywane poza zasięgiem dzieci.
- Elementy montażowe i drobne części mogą stanowić ryzyko zadławienia, dlatego należy je przechowywać w miejscu niedostępnym dla dzieci.
- Nie pozwalać dzieciom na samodzielne obsługiwanie urządzenia.

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.*