

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 M2010 / M2010W - monitor do wideodomofonu Vidos One

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

- Monitor należy montować zgodnie z instrukcją producenta, na stabilnej powierzchni lub w odpowiedniej puszcze montażowej.
- Podczas instalacji unikaj uszkodzenia przewodów sieciowych i zasilających; przewody powinny być prowadzone tak, aby nie były narażone na ściskanie, zagięcia lub przetarcia.
- Podłączenie do sieci elektrycznej i sieci Ethernet powinno być wykonane przez wykwalifikowany personel, zgodnie z obowiązującymi normami.
- Monitor wyposażony jest w moduł Wi-Fi; należy zapewnić odpowiednie zabezpieczenia sieci bezprzewodowej, aby uniknąć nieautoryzowanego dostępu.

3. Bezpieczeństwo użytkowania

- Nie używaj monitora, jeśli obudowa jest uszkodzona lub jeśli urządzenie nie działa prawidłowo.
- Nie demontuj ani nie modyfikuj urządzenia samodzielnie; wszelkie naprawy powinny być wykonywane przez autoryzowany serwis.
- Unikaj kontaktu monitora z wilgocią, ponieważ nie jest przeznaczony do pracy w warunkach mokrych lub wilgotnych.
- Nie używaj monitora pod wpływem alkoholu lub środków odurzających.
- Nie dotykaj ekranu mokrymi rękami, aby uniknąć uszkodzenia i porażenia prądem.

4. Bezpieczeństwo dzieci

- Monitor nie jest zabawką; trzymaj go poza zasięgiem dzieci.
- Małe elementy, takie jak śruby montażowe lub akcesoria, mogą stanowić ryzyko zadławienia.

5. Bezpieczeństwo sieci i danych

- Zabezpiecz sieć Wi-Fi odpowiednim hasłem i aktualizuj regularnie oprogramowanie monitora, aby chronić dane i prywatność użytkowników.
- Nie udostępniaj danych dostępowych do systemu osobom nieuprawnionym.
- W przypadku wykrycia nieautoryzowanego dostępu lub podejrzanej aktywności natychmiast odłącz monitor od sieci i skontaktuj się z serwisem.

6. Konserwacja i czyszczenie

- Przed czyszczeniem monitora odłącz go od zasilania.
- Używaj miękkiej, suchej ściereczki do czyszczenia ekranu i obudowy; nie stosuj środków chemicznych ani rozpuszczalników, które mogą uszkodzić powierzchnię.
- Regularnie sprawdzaj stan przewodów i złączy pod kątem uszkodzeń.

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.