

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 S100 - stacja bramowa Vidos IPX

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

- Wideodomofony serii Vidos IPX przeznaczone są do montażu wewnątrz i na zewnątrz budynków, jednak stacje bramowe powinny być instalowane w miejscach osłoniętych przed bezpośrednim działaniem wilgoci i ekstremalnych warunków atmosferycznych.
- Podczas montażu stacji bramowej i monitorów należy unikać uszkodzenia przewodów sieciowych oraz zasilających.
- Stacje bramowe i monitory należy montować stabilnie, używając oryginalnych elementów mocujących dostarczonych przez producenta.
- Nie modyfikować ani nie demontować urządzeń samodzielnie; wszelkie naprawy powinny być wykonywane przez wykwalifikowany personel.

3. Bezpieczeństwo zasilania i elektryki

- Podłączenie urządzeń do sieci elektrycznej i sieci komputerowej (RJ45) powinno być wykonane zgodnie z obowiązującymi normami i najlepiej przez specjalistę.
- Upewnij się, że napięcie zasilania jest zgodne z wymaganiami urządzenia (np. DC 12V lub PoE 802.3af dla monitorów).
- Nie uszkodzaj kabli sieciowych i zasilających, unikaj ich zginania, ściskania lub ciągnięcia za przewód.
- W przypadku uszkodzenia przewodów natychmiast odłącz urządzenie od zasilania i skontaktuj się z serwisem.
- Stosuj odpowiednie zabezpieczenia przeciwprzepięciowe, zwłaszcza przy podłączeniu do sieci zewnętrznej.

4. Bezpieczeństwo użytkowania

- Nie używaj urządzenia pod wpływem alkoholu lub środków odurzających.
- Nie dopuszczaj do kontaktu urządzenia z wilgocią, jeśli nie jest do tego przystosowane (np. monitory wewnętrzne).
- Nie blokuj otworów wentylacyjnych urządzeń, aby zapobiec przegrzaniu.
- W przypadku zauważenia nieprawidłowego działania, np. braku obrazu, dźwięku lub sygnałów alarmowych, natychmiast odłącz urządzenie i skontaktuj się z serwisem.
- Używaj funkcji zabezpieczeń, takich jak kod PIN, kody QR i czytniki RFID, aby ograniczyć dostęp osób nieuprawnionych.

5. Bezpieczeństwo dzieci

- Urządzenia nie są zabawkami. Trzymaj je poza zasięgiem dzieci, aby uniknąć przypadkowego uszkodzenia lub zadławienia małymi elementami.
- Małe elementy, takie jak przyciski czy karty RFID, mogą stanowić ryzyko zadławienia.

6. Konserwacja i czyszczenie

- Przed czyszczeniem urządzenia odłącz je od źródła zasilania.
- Do czyszczenia używaj miękkiej, suchej lub lekko wilgotnej szmatki. Nie stosuj agresywnych środków chemicznych, które mogą uszkodzić powierzchnię lub elektronikę.
- Regularnie sprawdzaj stan przewodów i złączy, aby zapobiec awariom.

7. Bezpieczeństwo sieci i danych

- Zabezpiecz sieć, do której podłączone są wideodomofony, stosując silne hasła i aktualizacje oprogramowania.
- Nie udostępniaj kodów PIN, kodów QR ani danych dostępowych osobom nieuprawnionym.
- Regularnie aktualizuj oprogramowanie urządzeń, aby zapewnić ochronę przed zagrożeniami cybernetycznymi.

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.