

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 Ajax IndoorCam - kamera Wi-Fi

1. Bezpieczeństwo montażu kamer IP

- Kamery montować wyłącznie na stabilnych i odpowiednio wytrzymałych powierzchniach, z użyciem elementów mocujących dobranych do rodzaju podłoża.
- Podczas instalacji unikać miejsc narażonych na silne drgania, wstrząsy lub możliwość przypadkowego uderzenia urządzenia.
- Nie prowadzić przewodów w sposób powodujący ryzyko ich przygniecenia, przecięcia lub potknięcia się użytkowników.
- Podczas wiercenia otworów montażowych upewnić się, że w ścianie nie znajdują się przewody elektryczne, rury lub inne instalacje.
- Kamery zewnętrzne montować zgodnie z przeznaczeniem producenta, w miejscach zapewniających ochronę przed zalewaniem wodą oraz nadmiernym zabrudzeniem.
- W przypadku montażu na wysokości stosować odpowiednie środki ochrony indywidualnej i stabilne narzędzia montażowe.

2. Bezpieczeństwo zasilania i podłączenia

- Przed podłączeniem sprawdzić zgodność napięcia oraz parametrów zasilacza z wymaganiami urządzenia.
- Nie używać uszkodzonych zasilaczy, przewodów ani wtyków zasilających.
- Podłączenia elektryczne wykonywać przy odłączonym zasilaniu.
- Nie przeciążać listew zasilających oraz gniazd elektrycznych wykorzystywanych do zasilania urządzeń monitoringu.
- Nie ciągnąć za przewód podczas odłączania urządzenia od zasilania.
- W przypadku kamer obsługujących PoE stosować wyłącznie kompatybilne urządzenia sieciowe i okablowanie o odpowiednich parametrach.
- Instalacje elektryczne oraz sieciowe powinny być wykonywane przez osoby posiadające odpowiednie kwalifikacje.

3. Bezpieczeństwo użytkowania kamer IP

- Używać kamer wyłącznie zgodnie z ich przeznaczeniem oraz warunkami pracy określonymi dla urządzeń wewnętrznych lub zewnętrznych.
- Nie zasłaniać obiektywu, otworów wentylacyjnych ani elementów odpowiedzialnych za odprowadzanie ciepła.
- Nie dotykać urządzenia mokrymi rękami ani nie obsługiwać go w warunkach zwiększonej wilgotności, jeśli kamera nie jest do tego przystosowana.

- Po przeniesieniu urządzenia z zimnego do ciepłego pomieszczenia odczekać do momentu całkowitego odparowania wilgoci powstałej wskutek kondensacji.
- Chronić kamerę przed silnymi wstrząsami, upadkiem oraz naciskiem mogącym uszkodzić obudowę lub układ optyczny.
- Nie kierować urządzeń wyposażonych w silne oświetlacze LED lub podczerwień bezpośrednio w oczy z bliskiej odległości.

4. Bezpieczeństwo sieci i komunikacji bezprzewodowej

- Po pierwszym uruchomieniu zmienić domyślne hasła dostępu na silne i unikalne.
- Regularnie aktualizować oprogramowanie urządzeń w celu ograniczenia ryzyka nieautoryzowanego dostępu.
- Nie udostępniać danych logowania osobom nieupoważnionym.
- Kamery Wi-Fi instalować w miejscach zapewniających stabilny sygnał sieci bezprzewodowej.
- Nie korzystać z niezabezpieczonych publicznych sieci do konfiguracji lub zdalnego dostępu do monitoringu.
- W przypadku kamer korzystających z sieci GSM lub LTE stosować wyłącznie kompatybilne karty SIM oraz chronić je przed uszkodzeniem mechanicznym.

5. Bezpieczeństwo eksploatacji akumulatorów i paneli solarnych

- Urządzenia wyposażone w akumulatory ładować wyłącznie przy użyciu zalecanych źródeł zasilania.
- Nie otwierać, nie przebijać ani nie podgrzewać akumulatorów.
- Nie stosować uszkodzonych lub zdeformowanych akumulatorów.
- Panele solarne montować w sposób stabilny, zapewniający odporność na działanie wiatru oraz przypadkowe poluzowanie mocowań.
- Nie przykrywać paneli solarnych podczas pracy oraz zapewnić im odpowiednią wentylację.
- Przewody paneli solarnych prowadzić w sposób zabezpieczający przed przetarciem i wpływem warunków atmosferycznych.

6. Bezpieczeństwo konserwacji i czyszczenia

- Przed czyszczeniem lub konserwacją odłączyć urządzenie od zasilania.
- Do czyszczenia obudowy i obiektywu stosować miękką, suchą lub lekko wilgotną ściereczkę.
- Nie używać agresywnych środków chemicznych, rozpuszczalników ani materiałów ściernych.
- Regularnie kontrolować stan przewodów, mocowań oraz szczelność elementów zewnętrznych.
- W przypadku zauważenia przegrzewania się urządzenia, zapachu spalenizny lub niestabilnej pracy natychmiast odłączyć zasilanie i skontaktować się z serwisem.
- Naprawy oraz ingerencję wewnątrz urządzenia powierzać wyłącznie wykwalifikowanym specjalistom.

7. Bezpieczeństwo dzieci i osób postronnych

- Kamery IP oraz akcesoria montażowe nie są zabawkami i powinny być przechowywane poza zasięgiem dzieci.
- Elementy montażowe, śruby, kołki, zaślepki oraz opakowania mogą stwarzać ryzyko zadławienia.
- Nie pozostawiać luźnych przewodów w miejscach dostępnych dla dzieci lub zwierząt.

- Nie pozwalać dzieciom na samodzielny montaż, demontaż ani konfigurację urządzeń elektrycznych.
- Nie używać urządzeń pod wpływem alkoholu, środków odurzających lub substancji ograniczających koncentrację.

8. Zagrożenia związane z bateriami

- UWAGA! Baterie należy używać tylko zgodnie z zasadami bezpieczeństwa, w przeciwnym razie mogą one spowodować pożar, wybuch lub prowadzić do obrażeń ciała bądź śmierci.
- Baterie należy trzymać z dala od dzieci.
- Połknięcie baterii może prowadzić do poważnych obrażeń ciała lub śmierci. W takim przypadku należy natychmiast zasięgnąć porady lekarza.
- Baterie należy wymieniać wyłącznie na takie same lub równoważnego typu.
- Nie wolno samodzielnie otwierać, modyfikować i naprawiać baterii.
- Wrzucenie baterii do ognia, zgniecenie lub przecięcie baterii może spowodować pożar lub wybuch.
- W przypadku rozszczelnienia i wycieku unikaj kontaktu z substancją chemiczną.
- Zużyte baterie należy natychmiast zutylizować w sposób przyjazny dla środowiska.

9. 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.

10. Prawidłowe usuwanie zużytego urządzenia

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

11. 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.