

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 NVMS Pro - platforma do zarządzania systemem monitoringu

1. Bezpieczeństwo instalacji i konfiguracji oprogramowania

- Oprogramowanie IPOX powinno być instalowane na komputerach spełniających minimalne wymagania sprzętowe i systemowe zalecane przez producenta.
- Instalację i konfigurację oprogramowania powinien przeprowadzać wykwalifikowany personel IT, aby uniknąć błędów mogących wpłynąć na bezpieczeństwo systemu monitoringu.
- Zaleca się stosowanie aktualnych wersji oprogramowania oraz regularne instalowanie dostępnych aktualizacji w celu eliminacji znanych luk bezpieczeństwa.
- Podczas konfiguracji systemu należy stosować silne hasła dostępu do kont użytkowników oraz ograniczać uprawnienia do niezbędnego minimum.

2. Bezpieczeństwo sieci i dostępu

- System monitoringu IPOX powinien być podłączony do zabezpieczonej sieci lokalnej z odpowiednimi zabezpieczeniami firewall i antywirusowymi.
- Dostęp do oprogramowania z poziomu przeglądarki internetowej i aplikacji mobilnej powinien być chroniony silnym uwierzytelnianiem oraz szyfrowaniem transmisji danych (np. SSL/TLS).
- Regularnie monitorować i aktualizować listę uprawnionych użytkowników, usuwając konta nieaktywnych lub nieuprawnionych osób.
- Nie udostępniać danych logowania osobom nieuprawnionym oraz unikać korzystania z publicznych sieci Wi-Fi podczas zdalnego dostępu do systemu.

3. Bezpieczeństwo użytkowania i eksploatacji

- Podczas pracy z oprogramowaniem należy unikać instalowania dodatkowych niezweryfikowanych wtyczek lub rozszerzeń, które mogą narazić system na ataki.
- W przypadku wykrycia nieprawidłowości w działaniu oprogramowania lub podejrzenia naruszenia bezpieczeństwa, należy niezwłocznie zgłosić to do administratora systemu lub serwisu technicznego.
- Nie należy używać oprogramowania pod wpływem alkoholu lub środków odurzających, aby uniknąć błędów obsługi mogących prowadzić do zagrożeń bezpieczeństwa.
- Zaleca się regularne wykonywanie kopii zapasowych konfiguracji i nagrań, aby zabezpieczyć dane przed utratą.

4. Bezpieczeństwo danych i prywatności

- Przechowywane dane w systemie monitoringu powinny być zabezpieczone przed nieautoryzowanym dostępem zgodnie z obowiązującymi przepisami o ochronie danych osobowych.
- W przypadku funkcji zliczania osób, generowania map ciepła i innych analiz, należy stosować się do zasad minimalizacji danych i przetwarzać tylko niezbędne informacje.

- Użytkownicy powinni być informowani o monitoringu zgodnie z obowiązującymi przepisami prawa.

5. Prawidłowe usuwanie zużytego urządzenia

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

6. 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.