

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 Klucz licencji AVB4212UX-10000S

1. Bezpieczeństwo aktywacji i konfiguracji licencji

- Przed aktywacją licencji należy upewnić się, że jest ona przeznaczona dla właściwego modelu urządzenia oraz zgodnej wersji oprogramowania.
- Aktywację i konfigurację funkcji sieciowych powinien wykonywać użytkownik posiadający odpowiednią wiedzę z zakresu konfiguracji urządzeń teleinformatycznych.
- Nie należy instalować ani aktywować licencji pochodzących z nieautoryzowanych źródeł lub o nieznanym pochodzeniu.
- Przed wprowadzeniem klucza licencyjnego zaleca się wykonanie kopii zapasowej aktualnej konfiguracji urządzenia.
- W trakcie aktywacji nie należy odłączać zasilania urządzenia ani przerywać połączenia sieciowego.

2. Bezpieczeństwo danych dostępowych i kluczy licencyjnych

- Klucze licencyjne, dane logowania oraz pliki aktywacyjne należy przechowywać w bezpiecznym miejscu, chroniąc je przed dostępem osób nieuprawnionych.
- Nie należy udostępniać kodów aktywacyjnych publicznie ani przysyłać ich niezabezpieczonymi kanałami komunikacji.
- Po zakończeniu konfiguracji zaleca się zmianę domyślnych haseł administratora urządzenia.
- W przypadku podejrzenia nieautoryzowanego użycia licencji należy niezwłocznie zmienić dane dostępowe i zweryfikować konfigurację systemu.

3. Bezpieczeństwo użytkowania systemów sieciowych

- Licencjonowane funkcje powinny być używane wyłącznie zgodnie z przeznaczeniem producenta urządzenia sieciowego.
- Nieprawidłowa konfiguracja funkcji sieciowych może powodować utratę komunikacji, ograniczenie wydajności lub nieautoryzowany dostęp do sieci.
- Należy regularnie aktualizować oprogramowanie urządzeń współpracujących z licencją w celu zapewnienia zgodności i bezpieczeństwa systemu.
- Nie należy modyfikować plików licencyjnych ani ingerować w mechanizmy zabezpieczeń producenta.
- Wszelkie zmiany konfiguracji sieciowej należy wykonywać ostrożnie, aby uniknąć przerw w działaniu infrastruktury.

4. 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.

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.