

*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 DS-K1T502DBWX-CQRE1 - terminal kontroli dostępu z kamerą, Wi-Fi, czytnikiem kodów QR oraz z zasilaniem PoE**

### **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 montażu i instalacji**

- Stacje bramowe należy montować na stabilnych powierzchniach, zapewniających odpowiednie mocowanie zgodnie z instrukcją producenta.
- Podczas instalacji należy unikać uszkodzenia przewodów sieciowych i zasilających, które mogą prowadzić do awarii lub zagrożenia porażeniem prądem.
- Nie należy modyfikować ani demontować urządzenia samodzielnie; wszelkie prace serwisowe powinny być wykonywane przez wykwalifikowany personel.
- Zaleca się montaż w miejscach osłoniętych przed bezpośrednim działaniem wilgoci, aby zapobiec uszkodzeniom elektronicznym.

### **3. Bezpieczeństwo elektryczne i zasilanie**

- Podłączaj urządzenie wyłącznie do sieci zasilającej o parametrach zgodnych z wymaganiami producenta.
- Stacje bramowe IP wyposażone są w interfejs RJ-45 do podłączenia sieci Ethernet; należy stosować odpowiednie kable i zabezpieczenia przed przepięciami.
- Podczas podłączania przewodów zasilających i sygnałowych należy zachować ostrożność, aby uniknąć zwarcia i uszkodzeń.
- Nie ciągnij ani nie uszkodzaj kabli; w przypadku uszkodzenia przewodów natychmiast odłącz urządzenie i skontaktuj się z serwisem.

### **4. Bezpieczeństwo użytkowania**

- Nie używaj urządzenia pod wpływem alkoholu lub środków odurzających.

- Nie dopuszczaj do kontaktu urządzenia z wodą ani innymi cieczami; w przypadku zalania natychmiast odłącz zasilanie.
- Nie blokuj otworów wentylacyjnych urządzenia, aby zapobiec przegrzaniu.
- Nie używaj uszkodzonych urządzeń; w przypadku zauważenia uszkodzeń natychmiast przerwij użytkowanie i skontaktuj się z serwisem.
- Nie modyfikuj oprogramowania ani sprzętu urządzenia bez zgody producenta.

## **5. Bezpieczeństwo dzieci**

- Urządzenia nie są zabawkami; należy trzymać je poza zasięgiem dzieci.
- Małe elementy, takie jak śruby czy zaślepki, mogą stanowić ryzyko zadławienia; przechowuj je w miejscach niedostępnych dla dzieci.

## **6. Konserwacja i serwis**

- Regularnie sprawdzaj stan urządzenia, zwracając uwagę na czystość obiektywu kamery oraz stan przewodów i mocowań.
- Do czyszczenia używaj miękkiej, suchej ściereczki; nie stosuj środków chemicznych ani rozpuszczalników.
- Wszelkie naprawy i wymiany części powinny być wykonywane wyłącznie przez autoryzowany serwis.

## **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.*