

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 Talon S130 - fotopułapka GSM 8Mpx 4G LTE z akumulatorem

1. Bezpieczeństwo montażu i instalacji

- Fotopułapkę należy montować stabilnie, na trwałych elementach, aby zapobiec jej upadkowi lub uszkodzeniu.
- Unikać instalacji w miejscach narażonych na bezpośrednie działanie wilgoci, deszczu lub silnych zmian temperatury, które mogą uszkodzić urządzenie.
- Podczas montażu należy uważać, aby nie uszkodzić przewodów, anteny GSM lub elementów czujników.
- Zaleca się montaż poza zasięgiem dzieci i zwierząt, aby uniknąć przypadkowego uszkodzenia lub manipulacji urządzeniem.

2. Bezpieczeństwo zasilania i baterii

- W przypadku modeli z akumulatorem, stosować wyłącznie oryginalne lub zalecane przez producenta źródła zasilania.
- Nie używać uszkodzonych baterii ani akumulatorów.
- Unikać kontaktu baterii z wilgocią oraz wysoką temperaturą, co może prowadzić do wycieku lub eksplozji.
- Przed wymianą baterii lub karty SIM wyłączyć urządzenie, aby uniknąć uszkodzenia elektroniki.

3. Bezpieczeństwo użytkowania i obsługi

- Nie należy demontować ani modyfikować urządzenia samodzielnie; wszelkie naprawy powinny być wykonywane przez autoryzowany serwis.
- Unikać bezpośredniego patrzenia w oświetlacz podczerwieni (IR LED), aby nie uszkodzić wzroku.
- Urządzenie nie jest zabawką; trzymać z dala od dzieci, aby uniknąć ryzyka zadławienia drobnymi elementami lub uszkodzenia sprzętu.
- Nie używać urządzenia pod wpływem alkoholu lub środków odurzających.
- Podczas obsługi karty SIM i kart pamięci stosować się do instrukcji producenta, aby uniknąć uszkodzenia danych lub sprzętu.

4. Bezpieczeństwo sieci i transmisji danych

- Podłączenie modułu GSM 4G LTE wymaga stosowania kart SIM zgodnych z urządzeniem i operatorem sieci.
- Chronić dane przesyłane przez urządzenie, stosując odpowiednie zabezpieczenia sieciowe i hasła dostępu do oprogramowania.
- Regularnie aktualizować oprogramowanie urządzenia, aby zapewnić bezpieczeństwo transmisji i ochronę przed nieautoryzowanym dostępem.

5. Konserwacja i czyszczenie

- Przed czyszczeniem urządzenia odłączyć je od zasilania i wyłączyć.
- Do czyszczenia obudowy używać miękkiej, suchej lub lekko wilgotnej szmatki; unikać środków chemicznych, które mogą uszkodzić powierzchnię lub elementy optyczne.
- Regularnie sprawdzać stan uszczelek i obudowy, aby zapewnić ochronę przed wilgocią i kurzem.

6. 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.

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.