

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 RKD32-SI-LIC - licencja na serwer do zarządzania depozytorem RKD

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 aktywacji i konfiguracji licencji

- Przed aktywacją licencji należy sprawdzić zgodność wersji oprogramowania, sprzętu oraz wymaganych modułów systemowych.
- Wprowadzanie kluczy licencyjnych i konfigurację systemu powinny wykonywać osoby posiadające odpowiednie uprawnienia administracyjne.
- Przed rozpoczęciem procesu aktywacji zaleca się wykonanie kopii zapasowej aktualnej konfiguracji systemu.
- Nie należy używać nieautoryzowanych narzędzi do modyfikacji lub aktywacji licencji.

3. Bezpieczeństwo danych i dostępu do systemu

- Klucze licencyjne, dane aktywacyjne oraz dane dostępowe należy przechowywać w sposób zabezpieczający przed nieuprawnionym dostępem.
- Dostęp do funkcji administracyjnych powinien być ograniczony wyłącznie do upoważnionych użytkowników.
- Po zakończeniu konfiguracji zaleca się stosowanie silnych haseł oraz regularną zmianę danych uwierzytelniających.
- Nie należy udostępniać danych licencyjnych osobom trzecim.

4. Bezpieczeństwo podczas aktualizacji oprogramowania

- Aktualizacje należy przeprowadzać zgodnie z dokumentacją producenta oraz procedurami obowiązującymi w danym systemie.
- Przed aktualizacją należy upewnić się, że urządzenia współpracujące są kompatybilne z nową wersją oprogramowania.

- W trakcie procesu aktualizacji nie należy wyłączać zasilania urządzeń ani przerywać komunikacji sieciowej.
- Po zakończeniu aktualizacji należy sprawdzić poprawność działania wszystkich funkcji systemu.

5. Bezpieczeństwo środowiska sieciowego

- System powinien pracować w odpowiednio zabezpieczonej sieci komputerowej chronionej przed nieautoryzowanym dostępem.
- Należy stosować aktualne mechanizmy zabezpieczeń sieciowych oraz regularnie aktualizować oprogramowanie systemowe.
- Nie należy instalować licencjonowanego oprogramowania na urządzeniach niespełniających wymagań bezpieczeństwa producenta.
- W przypadku połączeń zdalnych zaleca się korzystanie z szyfrowanych metod komunikacji.

6. Bezpieczeństwo użytkowania systemu

- Produkt należy wykorzystywać wyłącznie zgodnie z jego przeznaczeniem i zakresem funkcjonalnym określonym przez producenta.
- Nie należy samodzielnie modyfikować plików systemowych, mechanizmów licencjonowania ani ustawień mogących wpływać na stabilność działania systemu.
- W przypadku wystąpienia błędów działania należy skorzystać z pomocy wykwalifikowanego personelu lub wsparcia technicznego.

7. Bezpieczeństwo stanowiska komputerowego

- Komputer wykorzystywany do obsługi licencji powinien być zabezpieczony przed złośliwym oprogramowaniem i posiadać aktualne oprogramowanie ochronne.
- Należy regularnie monitorować stan nośników danych oraz wykonywać kopie zapasowe istotnych informacji konfiguracyjnych.
- W przypadku wykrycia uszkodzeń sprzętu komputerowego lub problemów z nośnikami danych należy wstrzymać operacje administracyjne do czasu usunięcia usterek.
- Po nagłej zmianie temperatury otoczenia urządzeń komputerowych należy odczekać do ustabilizowania warunków pracy przed ich uruchomieniem.

8. Bezpieczeństwo dzieci i osób nieuprawnionych

- Produkt nie jest przeznaczony do użytkowania przez dzieci.
- Dane licencyjne, nośniki zawierające klucze aktywacyjne oraz dokumentację należy przechowywać poza zasięgiem dzieci.
- Elementy opakowania oraz niewielkie akcesoria dołączone do produktu mogą stwarzać ryzyko zadławienia.
- Należy uniemożliwić dostęp do funkcji administracyjnych osobom nieuprawnionym.

9. Prawidłowe usuwanie zużytego urządzenia

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

10. 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.