Informacje i instrukcje dla użytkownika

Dokument dołączany do produktu z elementami cyfrowymi Aksel Sp. z o.o. zgodnie z wymogami unijnego Aktu o Cyberodporności (CRA).

Dane identyfikacyjne producenta

Aksel Sp. z o.o., jako producent rozwiązań cyfrowych, dostarcza niniejszy dokument w celu zapewnienia najwyższego poziomu cyberbezpieczeństwa oraz pełnej zgodności z horyzontalnymi wymaganiami Aktu o Cyberodporności (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847).

Nazwa Producenta	Aksel Sp. z o.o.
Adres Siedziby	ul. Lipowa 17/1, 44-207 Rybnik
E-mail	aksel@aksel.com.pl
Strona internetowa	www.aksel.com.pl
Nazwa produktu	
Numer seryjny/licencja	

Okres wsparcia w zakresie cyberbezpieczeństwa

Zgodnie z wymaganiami prawa unijnego, firma Aksel Sp. z o.o. deklaruje i gwarantuje minimalny okres wsparcia bezpieczeństwa wynoszący co najmniej 5 lat (zgodnie z regułą z art. 13 ust. 8 CRA). Przez ten czas użytkownik będzie otrzymywał bezpłatne aktualizacje zabezpieczeń usuwające zidentyfikowane podatności.

Rodzaj wsparcia:	Bezpłatne dostarczanie aktualizacji zabezpieczeń i poprawek podatności
Data zakończenia okresu wsparcia:	

Przeznaczenie, środowisko bezpieczeństwa i konfiguracja

Zgodnie z dokumentacją techniczną produktu.

Procedura instalacji aktualizacji i automatyczne poprawki

Aktualizacje zabezpieczeń dostarczane są bezpłatnie. Pakiety aktualizacyjne są podpisywane cyfrowo, a ich autentyczność oraz integralność są weryfikowane przed instalacją. O ile jest to technicznie wykonalne, poprawki bezpieczeństwa wydawane są oddzielnie od aktualizacji funkcjonalnych.

Sposób dystrybucji i instalacji aktualizacji zabezpieczeń zależy od charakterystyki produktu oraz środowiska, w którym jest on eksploatowany:

- W produktach posiadających dostęp do sieci publicznej aktualizacje zabezpieczeń są domyślnie pobierane i instalowane automatycznie.

- W produktach przeznaczonych do pracy ciągłej (24/7), w środowiskach o ograniczonym dostępie do sieci publicznych oraz w urządzeniach, które z natury nie mają dostępu do internetu, pakiety aktualizacji zabezpieczeń udostępniane są administratorowi systemu w postaci pliku, kanałem serwisowym.
- W aplikacjach mobilnych instalacja aktualizacji zabezpieczeń odbywa się zgodnie z mechanizmami platformy dystrybucyjnej (Google Play / App Store).

O dostępności każdej aktualizacji zabezpieczeń użytkownik jest informowany bez zbędnej zwłoki, wraz z informacją o usuwanej podatności, jej istotności oraz zalecanych działaniach.

Automatyczna instalacja aktualizacji zabezpieczeń jest ustawieniem domyślnym. W przypadku jej wyłączenia przez użytkownika lub administratora odpowiedzialność za terminowe wdrożenie aktualizacji spoczywa na użytkowniku.

W przypadku produktów wykonywanych na indywidualne zamówienie klienta zasady dotyczące dystrybucji i bezpłatności aktualizacji zabezpieczeń mogą zostać uregulowane odrębnie w umowie.

Bezpieczne wycofanie z użytku i trwałe usuwanie danych

Przed wycofaniem produktu z eksploatacji, odsprzedażą lub utylizacją, użytkownik ma obowiązek trwałego usunięcia wszystkich danych konfiguracyjnych, kluczy kryptograficznych oraz danych uwierzytelniających. W tym celu należy przeprowadzić procedurę resetu produktu zgodnie z instrukcją administracyjną, co uniemożliwia odzyskanie poufnych informacji.

Program Skoordynowanego Ujawniania Podatności

Aksel Sp. z o.o. aktywnie realizuje Program Skoordynowanego Ujawniania Podatności (Coordinated Vulnerability Disclosure). Zapraszamy badaczy bezpieczeństwa, partnerów biznesowych i klientów do zgłaszania wszelkich zauważonych anomalii lub luk bezpieczeństwa bezpośrednio do naszego Zespołu Cyberbezpieczeństwa.

Polityka skoordynowanego ujawniania podatności znajduje się na stronie www.aksel.com.pl/pl/cvd, www.aksel.com.pl/en/cvd

Dedykowany adres e-mail	cybersecurity@aksel.com.pl
Kontakt telefoniczny dla incydentów krytycznych	+48 601 457 600, +48 32 42 95 100

Aksel Sp. z o.o. zobowiązuje się do niepodejmowania kroków prawnych ani dyscyplinarnych wobec osób, które zgłaszają podatności w dobrej wierze, dając naszej firmie czas na zdiagnozowanie i przygotowanie poprawki.

Wzór formularza zgłoszenia podatności

Pole formularza	Opis i wymagane dane techniczne
Identyfikacja zgłaszającego	Imię i nazwisko, organizacja, e-mail kontaktowy (możliwe zgłoszenie anonimowe).
Dane o produkcie	Nazwa produktu Aksel, model, wersja sprzętowa (HW) i oprogramowania (SW).
Szczegółowy opis podatności	Typ podatności (np. przepełnienie bufora, błąd uwierzytelniania).
Kroki do odtworzenia	Instrukcja krok po kroku lub skrypt wykazujący istnienie podatności (Proof of Concept).
Potencjalny wpływ	Określenie konsekwencji (np. zdalne wykonanie kodu, odmowa usługi DoS).