User Information and Instructions

Document included with Aksel Sp. z o.o. products containing digital elements, in accordance with the requirements of the EU Cyber Resilience Act (CRA)

Manufacturer Identification Information

Aksel Sp. z o.o., as a manufacturer of digital solutions, provides this document to ensure the highest level of cybersecurity and full compliance with the horizontal requirements of the Cyber Resilience Act (Regulation (EU) 2024/2847 of the European Parliament and of the Council).

Manufacturer Name	Aksel Sp. z o.o.
Registered Office Address	17/1 Lipowa, 44-207 Rybnik
Email	aksel@aksel.com.pl
Website	www.aksel.com.pl
Product Name	
Serial Number/License	

Cybersecurity Support Period

In accordance with EU law, Aksel Sp. z o.o. declares and guarantees a minimum cybersecurity support period of at least 5 years (in accordance with the rule set forth in Article 13(8) of the CRA). During this time, the user will receive free security updates that address identified vulnerabilities.

Type of support:	Free provision of security updates and vulnerability patches
End date of the support period:	

Intended use, security environment, and configuration

As specified in the product's technical documentation.

Update installation procedure and automatic patches

Security updates are provided free of charge. Update packages are digitally signed, and their authenticity and integrity are verified prior to installation. Wherever technically feasible, security patches are released separately from functional updates.

The method of distributing and installing security updates depends on the product's characteristics and the environment in which it operates:

- For products with public network access, security updates are downloaded and installed automatically by default.

- For products designed for continuous operation (24/7), those in environments with limited public network access, and devices that inherently lack internet access, security update packages are made available to the system administrator as a file via a service channel.
- For mobile applications, security updates are installed in accordance with the mechanisms of the distribution platform (Google Play / App Store).

Users are notified of the availability of each security update without undue delay, along with information regarding the vulnerability being addressed, its severity, and recommended actions.

Automatic installation of security updates is the default setting. If this feature is disabled by the user or administrator, the responsibility for the timely implementation of updates rests with the user.

For custom-made products, the terms regarding the distribution and provision of security updates free of charge may be stipulated separately in the contract.

Secure Decommissioning and Permanent Data Deletion

Before decommissioning, reselling, or disposing of the product, the user is required to permanently delete all configuration data, cryptographic keys, and authentication data. To do this, perform the product reset procedure in accordance with the administrative instructions, which prevents the recovery of confidential information.

Coordinated Vulnerability Disclosure Program

Aksel Sp. z o.o. actively implements the Coordinated Vulnerability Disclosure Program. We invite security researchers, business partners, and customers to report any observed anomalies or security vulnerabilities directly to our Cybersecurity Team.

The Coordinated Vulnerability Disclosure Policy can be found at

www.aksel.com.pl/pl/cvd, www.aksel.com.pl/pl/cvd

Dedicated email address	cybersecurity@aksel.com.pl
Phone contact for critical incidents	+48 601 457 600, +48 32 42 95 100

Aksel Sp. z o.o. commits to not taking any legal or disciplinary action against individuals who report vulnerabilities in good faith, allowing our company time to diagnose the issue and prepare a fix.

Vulnerability Report Form Template

Form field	Description and required technical details
Reporter identification	First and last name, organization, contact email (anonymous reports are allowed anonymous).
Product information	Product name: Aksel, model, hardware (HW) and software (SW).
Detailed description of the vulnerability	Vulnerability type (e.g., buffer overflow, authentication error).
Steps to reproduce	Step-by-step instructions or a script demonstrating the existence of the vulnerability (Proof of Concept).
Potential impact	Description of the consequences (e.g., remote code execution, denial of service (DoS)).