Security Vulnerability Reporting and Handling Policy

We treat the security of our solutions — from radio communication systems to dispatch software and rail transport solutions — as a top priority. The document below describes how we receive, assess and handle reports of vulnerabilities relating to our products and infrastructure, and the principles governing our cooperation with those who report them.

Who this policy applies to and what it covers

This document covers all products and services offered by Aksel Sp. z o.o. that contain digital components — regardless of whether they were developed by us or are merely maintained or operated by us — as well as the company's infrastructure, to which reports are submitted via the official channels indicated below.
However, the following fall outside its scope:

- solutions and services provided by third-party suppliers which Aksel Sp. z o.o. neither owns nor administers,
- situations arising from a customer's individual configuration or from the incorrect use of the product.

When we consider a report to be a valid vulnerability

When classifying a report as a valid vulnerability, we apply three criteria:

- the reported issue must relate to a specific product or element of Aksel Sp. z o.o.'s infrastructure,
- the report should highlight information that is not in the public domain,
- it must not be based solely on the results of an automated scan without accompanying documentation — the vulnerability must be exploitable under real-world operating conditions.

How to report a vulnerability

We accept reports via a dedicated, secure channel:

Email: cybersecurity@aksel.com.pl
Contact form:
https://www.aksel.com.pl/pl/cvd
https://www.aksel.com.pl/en/cvd
https://www.interloco.com.pl/cvd
https://conselplus.com/cvd

A vulnerability report should include:

- a description of the problem, including the steps required to reproduce it,
- the name, version and environment of the affected product,
- illustrative materials — e.g. proof of concept, screenshots, logs.

You may submit a report anonymously. However, please be aware that without contact details, we will not be able to confirm receipt of your report or provide updates on its status.

What happens after a report is submitted

Stage	What we do
Confirmation	We confirm receipt of a valid report within the timeframe set out in the EU's Cyber Resilience Act.
Analysis	We assess the report in terms of its scale, impact and actual threat.
Remediation	The relevant technical team prepares and tests a fix or a mitigating measure.
Feedback	We inform the reporter of the progress of the work and, where appropriate, of the planned date of public disclosure.
Closure	Once the fix has been implemented, we document the issue internally and, where appropriate, publish information about it — including the name of the reporter, provided they have given their consent.

What we do not treat as a vulnerability

- problems caused by incorrect configuration or improper or risky use of the product by the user,
- reports concerning third-party components over which we have no control,
- purely theoretical issues or those of negligible practical significance,
- raw results from automated scanners without a description or reproducible evidence.

Our commitment to researchers (safe harbour)

We value honest cooperation with security professionals. Provided the reporter acts in accordance with this policy and in good faith, Aksel Sp. z o.o. will not take legal action against them in connection with the discovery and reporting of a vulnerability.
In return, we expect the researcher to take care not to infringe the privacy of third parties, disrupt the operation of our services or cause data loss whilst conducting their tests.

Updates to this document

This policy forms part of Aksel Sp. z o.o.'s broader Coordinated Vulnerability Disclosure Policy. We review it at least once a year, as well as in the event of significant organisational or legal changes.

Contact

Cybersecurity Team — Aksel Sp. z o.o.
Email: cybersecurity@aksel.com.pl
Website: aksel.com.pl/cvd