Coordinated Vulnerability Disclosure

How to report a security weakness to us, and what we promise.

VERSION 2 17 NOVEMBER 2026 ENGLISH PUBLIC

01 Scope

This policy covers the website avvi.ch and our products Adhara, HF4, Feint and REN, in versions you obtained lawfully. It does not cover systems that our customers or others run.

In this document, “AVVI”, “we” and “us” mean the company named in the imprint on avvi.ch/legal and the companies in its group.

02 How to report

Use the contact form at avvi.ch/contact and choose “Security issue”. Please include:

- the product and version, or the web address, that is affected;
- what the weakness is and what an attacker could do with it;
- the steps to reproduce it, with any proof of concept;
- how you would like to be credited, if at all.

Do not send real personal data or secrets in your report. If you need a safer way to share details, say so and we will arrange one.

03 What we promise

- We confirm receipt within 5 working days.
- We give you our first assessment within 10 working days and keep you informed until the weakness is fixed.
- We aim to fix valid weaknesses within 90 days, sooner when they are serious, and agree a later date with you if a fix takes longer.
- We publish an advisory on our website when a fix is available, and credit you if you wish.
- Where the law requires it, we notify the competent authorities of an actively exploited vulnerability, with an early warning within 24 hours.

04 Safe harbour

If you act in good faith and follow this policy, we will not take legal action against you for your research. That means you:

- test only avvi.ch or a copy of a product you obtained lawfully;
- do not access, change or keep other people's data, and stop as soon as you find a weakness;
- do not disrupt any service, and do no denial of service, social engineering or physical attacks;
- give us reasonable time to fix the weakness before you make it public, normally 90 days.

This does not permit anything the law forbids. You may also report to a national computer security incident response team (CSIRT).

05 Not in scope

Reports from automated scanners without a demonstrated impact, missing security headers without an exploit, spam, and weaknesses in third-party services we do not control.

06 security.txt

Our contact details for security reports are also published at avvi.ch/.well-known/security.txt.

07 Ownership

Management owns this policy and reviews it every year.

Version 2 replaces version 1 of 1 November 2026. AVVI now makes software only; the parts about our own interceptor are removed.

The current version of this document is published at avvi.ch/docs/avvi-vulnerability-disclosure.pdf. If you have a question about it, write to us through avvi.ch/contact.