Coordinated Vulnerability Disclosure Policy

This Coordinated Vulnerability Disclosure (CVD) policy describes how our customers can report vulnerabilities to us and how we respond to them. It meets the transparency requirements of the Cyber Resilience Act (CRA), based on the prEN 40000-1-3 Standard.

Principles and Commitment

We value the work of our customers. If you discover a vulnerability in our products, we ask that you report it to us confidently. In return, we commit to transparent, cooperative collaboration and will refrain from taking legal action, provided you adhere to this policy.

Secure Reporting Channels

Please send all reports on security vulnerabilities directly to our after-sales service team:
E-mail: service@wandfluh.com

- Encryption: A PGP key can be provided for highly sensitive vulnerabilities or data
- Content of the report: Product name, item number, software version, a description of the vulnerability, and steps to reproduce it (proof of concept).

Our response timeline (SLA)

We are committed to clear deadlines throughout the entire process:

- Within 5 working days: We will acknowledge receipt of the report
- Within a further 10 working days: We will review the report and provide initial technical feedback.
- Regular updates: We will provide an update on the status of the fix at least every 30 working days.

Rules of Engagement

To benefit from protection against legal action (Safe Harbor), you must comply with the following rules:

- None: Do not exploit the vulnerability to steal data, destroy systems, or block services.
- Confidentiality: Do not publish any details of the vulnerability before we have released a security update (Coordinated Disclosure).
- Data protection: Do not access customer data. If you accidentally come across such data, stop the test immediately and report this straight away.
- Integrity of the test environment: Customers may only carry out tests on their own systems or in dedicated test environments. The operation of other customers' systems must not be disrupted at any time.

Remediation

Following successful verification, we will promptly develop a patch or workaround.