# Coordinated Vulnerability Disclosure Policy

Diese Richtlinie für die koordinierte Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure - CVD) beschreibt, wie unsere Kunden Schwachstellen an uns melden können und wie wir darauf reagieren. Sie erfüllt die Transparenzanforderungen des Cyber Resilience Act (CRA) angelehnt an den Standard prEN 40000-1-3.

## Grundsatz und Versprechen

Wir schätzen die Arbeit unserer Kunden. Wenn Sie eine Schwachstelle in unseren Produkten finden, bitten wir Sie, diese vertraulich an uns zu melden. Im Gegenzug verpflichten wir uns zu einer transparenten, kooperativen Zusammenarbeit und verzichten auf rechtliche Schritte, solange Sie sich an diese Richtlinie halten.

## Sichere Meldekanäle

Bitte senden Sie alle Berichte über Sicherheitslücken direkt an unseren Kundendienst:
E-Mail: service@wandfluh.com

- Verschlüsselung: Bei hochsensiblen Schwachstellen oder Daten kann ein PGP-Schlüssel bereitgestellt werden
- Inhalt der Meldung: Produktname, Artikelnummer, Softwareversion, eine Beschreibung der Lücke sowie Schritte zum Reproduzieren (Proof of Concept).

## Unser Zeitplan für die Reaktion (SLA)

Wir verpflichten uns zu klaren Fristen während des gesamten Prozesses:

- Innerhalb von 5 Werktagen: Wir bestätigen den Eingang der Meldung
- Innerhalb von 10 weiteren Werktagen: Wir prüfen die Meldung und senden eine erste technische Rückmeldung.
- Regelmässige Updates: Wir informieren spätestens alle 30 Werktage über den aktuellen Status der Behebung.

## Verhaltensregeln (Rules of Engagement)

Um Schutz vor rechtlichen Schritten (Safe Harbor) zu geniessen, müssen Sie folgende Regeln einhalten:

- Kein Schaden: Nutzen Sie die Schwachstelle nicht aus, um Daten zu stehlen, Systeme zu zerstören oder Dienste zu blockieren.
- Vertraulichkeit: Veröffentlichen Sie keine Details zur Schwachstelle, bevor wir ein Sicherheitsupdate bereitgestellt haben (Coordinated Disclosure).
- Datenschutz: Greifen Sie nicht auf Kundendaten zu. Wenn Sie versehentlich darauf stossen, brechen Sie den Test ab und melden Sie dies sofort.
- Integrität der Testumgebung: Kunden dürfen Prüfungen ausschliesslich an ihren eigenen Systemen oder dedizierten Testumgebungen durchführen. Der Betrieb der Systeme anderer Kunden darf dadurch zu keinem Zeitpunkt beeinträchtigt werden.

## Behebung

Nach erfolgreicher Verifizierung entwickeln wir zeitnah einen Patch oder Workaround.