Coordinated Vulnerability Disclosure Policy

Instrument Systems GmbH

Version 1.0 | Stand: August 2026

1. Einleitung und Zweck

Diese Coordinated Vulnerability Disclosure Policy (CVD-Policy) legt fest, wie Instrument Systems mit Meldungen über Sicherheitslücken in eigenen Produkten, Systemen und digitalen Diensten umgeht. Sie richtet sich an Sicherheitsforscher, Kunden, Partner und alle weiteren Personen, die eine mögliche Schwachstelle entdecken und melden möchten.

Diese Policy dient der Umsetzung der Anforderungen an die koordinierte Offenlegung von Schwachstellen gemäß dem Cyber Resilience Act (Verordnung (EU) 2024/2847), Anhang I Teil II, sowie international anerkannter Standards wie ISO/IEC 29147 (Vulnerability Disclosure) und ISO/IEC 30111 (Vulnerability Handling Processes).

2. Geltungsbereich

Diese Policy gilt für Schwachstellen in:

- Produkten von Instrument Systems, einschließlich Hardware mit digitalen Elementen,
- zugehöriger Software, Firmware und eingebetteten Komponenten,
- digitalen Diensten, Webanwendungen und Schnittstellen, die von Instrument Systems bereitgestellt oder betrieben werden,
- Drittkomponenten, die in den genannten Produkten und Diensten enthalten sind, soweit die Schwachstelle über ein Produkt von Instrument Systems beobachtet wurde.

Nicht erfasst sind Systeme, Netzwerke oder Dienste Dritter, die nicht von Instrument Systems bereitgestellt oder betrieben werden, auch wenn Produkte von Instrument Systems darin eingesetzt werden.

3. Erlaubte Test- und Meldeaktivitäten (Safe Harbor)

Instrument Systems ermutigt zur verantwortungsvollen Sicherheitsforschung. Gegen Personen, die eine Schwachstelle in gutem Glauben und im Einklang mit dieser Policy melden und die nachfolgenden Bedingungen einhalten, beabsichtigt Instrument Systems grundsätzlich nicht, Strafanzeige zu erstatten oder sonstige strafrechtliche Schritte zu veranlassen Diese Zusicherung gilt nicht bei vorsätzlichem oder böswilligem Verhalten oder wenn die nachfolgend genannten Bedingungen

nicht eingehalten werden. Gesetzliche Verpflichtungen von Instrument Systems, insbesondere gegenüber Behörden, bleiben unberührt.

- Tests werden auf den Umfang beschränkt, der zur Verifikation der Schwachstelle notwendig ist.
- Es werden keine Daten Dritter oder von Instrument Systems eingesehen, verändert, kopiert, gelöscht oder exfiltriert, die über das zur Bestätigung der Schwachstelle erforderliche Minimum hinausgehen.
- Es werden keine Systeme, Dienste oder die Verfügbarkeit von Produkten beeinträchtigt (unter anderem keine Denial-of-Service-Tests).
- Es erfolgen keine Angriffe auf physische Sicherheit, Social Engineering, Phishing gegenüber Mitarbeitenden, Kunden oder Dritten.
- Die Schwachstelle wird über den in Abschnitt 4 genannten Kanal gemeldet, bevor eine öffentliche Offenlegung erfolgt.
- Instrument Systems wird angemessene Zeit und Gelegenheit zur Prüfung und Behebung gemäß Abschnitt 7 eingeräumt, bevor Informationen veröffentlicht werden.
- Es werden keine Dritten (z. B. Kunden von Instrument Systems) durch die Testaktivität beeinträchtigt.

4. Meldeweg

Schwachstellenmeldungen sind zu richten an:

vulnerability@instrumentsystems.com

Bevorzugte Sprachen: Englisch oder Deutsch.

Ergänzende Kontakt- und Verifikationsinformationen sind in der Datei security.txt unter der Domain von Instrument Systems veröffentlicht.

Zu den gewünschten Angaben einer Meldung siehe die begleitende Webseite zur Schwachstellenmeldung.

5. Annahme und Bewertung von Meldungen

Nach Eingang einer Meldung geht Instrument Systems wie folgt vor:

1. **Eingang und Dokumentation:** Jede Meldung wird erfasst, dokumentiert und einer internen Fallnummer zugeordnet.
2. **Erstbestätigung:** Bei vorhandener Kontaktmöglichkeit erhält die meldende Person innerhalb von fünf Arbeitstagen eine erste, nicht automatisierte Rückmeldung.
3. **Triage und Bewertung:** Die gemeldete Schwachstelle wird durch zuständige interne Stellen geprüft, auf Plausibilität und Reproduzierbarkeit hin bewertet und hinsichtlich ihrer technischen Auswirkung eingeordnet, etwa anhand eines anerkannten Bewertungsschemas wie CVSS.
4. **Rückfragen:** Bei Bedarf an zusätzlichen Informationen kontaktiert Instrument Systems die meldende Person über den angegebenen Kontaktweg.

5. **Remediation-Planung:** Bei bestätigten Schwachstellen legt Instrument Systems Maßnahmen und einen Zeitrahmen zur Behebung fest, priorisiert nach Schweregrad und Ausnutzbarkeit.
6. **Umsetzung:** Instrument Systems entwickelt und veröffentlicht geeignete Abhilfemaßnahmen, zum Beispiel Sicherheitsupdates, Patches oder Konfigurationsanleitungen.
7. **Rückmeldung an die meldende Person:** Sofern eine Kontaktmöglichkeit vorliegt, wird die meldende Person über den Status und nach erfolgter Behebung informiert.

6. Bearbeitungs- und Behebungsfristen

Die Bearbeitungszeit richtet sich nach Komplexität, Nachvollziehbarkeit und technischer Auswirkung der gemeldeten Schwachstelle. Instrument Systems ist bestrebt:

- kritische Schwachstellen mit hoher Ausnutzbarkeit vorrangig und ohne unangemessene Verzögerung zu bearbeiten,
- meldende Personen bei absehbaren Verzögerungen über den Fortschritt zu informieren,
- Schwachstellen innerhalb eines angemessenen Zeitraums zu beheben, der sich an der Kritikalität orientiert.

Sofern gesetzlich vorgeschrieben, etwa im Rahmen aktiv ausgenutzter Schwachstellen gemäß den Meldepflichten des Cyber Resilience Act, erfolgen zusätzlich die erforderlichen Meldungen an die zuständigen Behörden innerhalb der dort vorgesehenen Fristen.

7. Koordinierte Offenlegung

Instrument Systems bittet meldende Personen, Informationen zu einer gemeldeten Schwachstelle bis zur Behebung vertraulich zu behandeln.

Eine öffentliche Offenlegung soll grundsätzlich erst erfolgen, nachdem:

- eine Abhilfemaßnahme verfügbar ist, oder
- eine angemessene Frist verstrichen ist, die zwischen Instrument Systems und der meldenden Person abgestimmt wurde und sich in der Regel auf **90 Kalendertage ab Eingang der Meldung beläuft**. Sofern eine nachvollziehbare und verifizierte Begründung vorliegt, kann dieser Zeitraum in enger Abstimmung mit der meldenden Person sowie dem zuständigen nationalen CSIRT einmalig um weitere 90 Kalendertage verlängert werden.

Instrument Systems ist bestrebt, den Zeitpunkt und Inhalt einer öffentlichen Veröffentlichung, etwa in Form eines Sicherheitshinweises (Security Advisory), mit der meldenden Person abzustimmen.

Sofern eine unmittelbare Gefährdung von Nutzern besteht, kann Instrument Systems eine frühere Veröffentlichung vornehmen, auch ohne vollständige Behebung, um Anwender in die Lage zu versetzen, Schutzmaßnahmen zu ergreifen.

8. Anerkennung meldender Personen

Instrument Systems würdigt den Beitrag von Personen, die verantwortungsvoll Schwachstellen melden. Auf Wunsch kann die meldende Person in einem veröffentlichten Sicherheitshinweis namentlich genannt werden. Ohne ausdrückliche Zustimmung erfolgt keine Namensnennung.

Instrument Systems bietet derzeit kein Bug-Bounty-Programm mit finanzieller Vergütung an.

9. Informationsaustausch mit Dritten

Instrument Systems ergreift geeignete Maßnahmen, um relevante Informationen über Schwachstellen mit betroffenen Stellen auszutauschen, unter anderem:

- mit Lieferanten und Herstellern betroffener Drittkomponenten,
- mit zuständigen nationalen oder europäischen Behörden, soweit gesetzlich vorgeschrieben,
- mit betroffenen Kunden, sofern dies zur Risikominimierung erforderlich ist.

Die Weitergabe erfolgt im Rahmen der gesetzlichen Vorgaben unter Wahrung der Vertraulichkeit der meldenden Person, soweit nicht ausdrücklich anders vereinbart.

10. Vertraulichkeit und Datenschutz

Von meldenden Personen übermittelte personenbezogene Daten, insbesondere Kontaktdaten, werden ausschließlich zur Bearbeitung der Meldung und zur Kommunikation im Rahmen des Vulnerability-Handling-Prozesses verwendet. Eine Weitergabe an Dritte erfolgt nur, soweit dies zur Bearbeitung der Meldung erforderlich oder gesetzlich vorgeschrieben ist.

Weitere Informationen zur Verarbeitung personenbezogener Daten im Zusammenhang mit Schwachstellenmeldungen finden Sie in unserer Datenschutzerklärung. https://www.instrumentsystems.com/de/datenschutzhinweise

11. Nicht erfasste Anfragen

Diese Policy und der zugehörige Meldeweg dienen ausschließlich der Meldung von Cybersicherheits-Schwachstellen. Allgemeine Support-Anfragen, Servicefälle, Produktfragen oder Vertriebsanfragen sind über die regulären Kontaktwege von Instrument Systems zu stellen.

12. Änderungen dieser Policy

Instrument Systems behält sich vor, diese Policy bei Bedarf zu aktualisieren, um sie an geänderte rechtliche Anforderungen, interne Prozesse oder Erkenntnisse aus der Praxis anzupassen. Die jeweils aktuelle Fassung wird auf der Webseite von Instrument Systems veröffentlicht.

13. Kontakt

Für Fragen zu dieser Policy oder zur Meldung einer Schwachstelle:

vulnerability@instrumentsystems.com

Weitere Informationen finden Sie auf der Webseite zur Meldung von Cybersicherheits-Schwachstellen sowie in der veröffentlichten security.txt.