Coordinated Vulnerability Disclosure Policy

Instrument Systems GmbH

Version 1.0 | As of: August 2026

1. Introduction and Purpose

This Coordinated Vulnerability Disclosure Policy (CVD Policy) sets out how Instrument Systems handles reports of security vulnerabilities in its own products, systems, and digital services. It is addressed to security researchers, customers, partners, and any other individuals who discover and wish to report a potential vulnerability.

This policy serves to implement the requirements for the coordinated disclosure of vulnerabilities under the Cyber Resilience Act (Regulation (EU) 2024/2847), Annex I Part II, as well as internationally recognized standards such as ISO/IEC 29147 (Vulnerability Disclosure) and ISO/IEC 30111 (Vulnerability Handling Processes).

2. Scope

This policy applies to vulnerabilities in:

- Instrument Systems products, including hardware with digital elements,
- associated software, firmware, and embedded components,
- digital services, web applications, and interfaces provided or operated by Instrument Systems,
- third-party components contained in the products and services referenced above, insofar as the vulnerability was observed via an Instrument Systems product.

This policy does not cover systems, networks, or services of third parties that are not provided or operated by Instrument Systems, even where Instrument Systems products are used within them.

3. Permitted Testing and Reporting Activities (Safe Harbor)

Instrument Systems encourages responsible security research. Instrument Systems generally does not intend to file a criminal complaint or otherwise initiate criminal-law measures against individuals who report a vulnerability in good faith and in accordance with this Policy and comply with the following conditions. This assurance does not apply in cases of intentional or malicious conduct or where the conditions set out below are not complied with. Any legal obligations of Instrument Systems, in particular vis-à-vis competent authorities, remain unaffected.

- Testing is limited to the extent necessary to verify the vulnerability.
- No data belonging to third parties or to Instrument Systems is accessed, modified, copied, deleted, or exfiltrated beyond the minimum required to confirm the vulnerability.
- No systems, services, or the availability of products are disrupted (including, but not limited to, denial-of-service testing).
- No attacks are carried out against physical security, and no social engineering or phishing is directed at employees, customers, or third parties.
- The vulnerability is reported through the channel specified in Section 4 before any public disclosure takes place.
- Instrument Systems is given reasonable time and opportunity to review and remediate the vulnerability in accordance with Section 7 before information is published.
- No third parties (e.g., customers of Instrument Systems) are affected by the testing activity.

4. Reporting Channel

Vulnerability reports should be sent to:

vulnerability@instrumentsystems.com

Preferred languages: English or German.

Supplementary contact and verification information is published in the security.txt file under the Instrument Systems domain.

For details on the information a report should include, please refer to the accompanying vulnerability reporting webpage.

5. Intake and Assessment of Reports

Upon receiving a report, Instrument Systems proceeds as follows:

1. **Intake and documentation:** Every report is logged, documented, and assigned an internal case number.
2. **Initial acknowledgment:** Where contact details are available, the reporting person receives an initial, non-automated response within five business days.
3. **Triage and assessment:** The reported vulnerability is reviewed by the responsible internal parties, assessed for plausibility and reproducibility, and classified with respect to its technical impact, for example using a recognized scoring scheme such as CVSS.
4. **Follow-up questions:** If additional information is needed, Instrument Systems contacts the reporting person via the provided contact details.
5. **Remediation planning:** For confirmed vulnerabilities, Instrument Systems defines remediation measures and a timeframe, prioritized according to severity and exploitability.

6. **Implementation:** Instrument Systems develops and releases appropriate remediation measures, such as security updates, patches, or configuration guidance.
7. **Feedback to the reporting person:** Where contact details are available, the reporting person is informed of the status and notified once the vulnerability has been remediated.

6. Processing and Remediation Timeframes

Processing time depends on the complexity, reproducibility, and technical impact of the reported vulnerability. Instrument Systems is committed to:

- prioritizing and addressing critical vulnerabilities with high exploitability without undue delay,
- keeping reporting persons informed of progress in the event of foreseeable delays,
- remediating vulnerabilities within a reasonable timeframe commensurate with their criticality.

Where legally required, for example in connection with actively exploited vulnerabilities under the reporting obligations of the Cyber Resilience Act, the necessary notifications to the competent authorities are made within the timeframes prescribed there.

7. Coordinated Disclosure

Instrument Systems asks reporting persons to keep information about a reported vulnerability confidential until it has been remediated.

Public disclosure should generally take place only after:

- a remediation measure is available, or
- a reasonable period has elapsed, which as a general rule amounts to 90 calendar days from receipt of the report. Provided a valid and verified justification exists, this period may be extended once by a further 90 calendar days, in close consultation with the reporting person and the competent national CSIRT.

Instrument Systems seeks to coordinate the timing and content of any public disclosure, for example in the form of a security advisory, with the reporting person.

Where there is an imminent risk to users, Instrument Systems may issue an earlier disclosure, even without a complete remediation, to enable users to take protective measures.

8. Recognition of Reporting Persons

Instrument Systems values the contribution of individuals who responsibly report vulnerabilities. Upon request, the reporting person may be named in a published security advisory. No attribution is made without express consent.

Instrument Systems does not currently offer a bug bounty program with financial compensation.

9. Information Sharing with Third Parties

Instrument Systems takes appropriate measures to share relevant vulnerability information with affected parties, including:

- suppliers and manufacturers of affected third-party components,
- competent national or European authorities, where legally required,
- affected customers, where necessary to mitigate risk.

Disclosure is carried out to the extend permitted by law while preserving the confidentiality of the reporting person, unless expressly agreed otherwise.

10. Confidentiality and Data Protection

Personal data submitted by reporting persons, in particular contact details, is used exclusively to process the report and to communicate within the vulnerability handling process. Disclosure to third parties occurs only where necessary to process the report or where legally required.

Further information on the processing of personal data in connection with vulnerability reports can be found in our Privacy Policy. https://www.instrumentsystems.com/en/privacy-policy

11. Out of Scope Requests

This policy and the associated reporting channel are intended exclusively for reporting cybersecurity vulnerabilities. General support requests, service cases, product inquiries, or sales inquiries should be directed to Instrument Systems' regular contact channels.

12. Changes to This Policy

Instrument Systems reserves the right to update this policy as needed to reflect changes in legal requirements, internal processes, or practical experience. The current version is published on the Instrument Systems website.

13. Contact

For questions about this policy or to report a vulnerability:

vulnerability@instrumentsystems.com

Further information is available on the vulnerability reporting webpage as well as in the published security.txt.