Coordinated Vulnerability Disclosure Policy (CVD Policy) | BRUKER

Must at least be reviewed annually.		
Version: 0.1	**Date: 2026-06-02**	**Initial publication**

- Coordinated Vulnerability Disclosure Policy (CVD policy)
  - Overview
  - Products and services in scope
  - Scope of vulnerability disclosure
  - Exclusions from the scope
  - Reporting
  - What we expect from you
  - Safe harbor
  - Limitation of liability
  - What you can expect from us
  - Formal case closure
  - Disclaimer

Coordinated Vulnerability Disclosure Policy (CVD policy)

Overview

Bruker Corporation (“Bruker”, “we” or “our”) values the security of its products, systems and services. We recognize the importance of collaboration with the broader security community and value the efforts of external stakeholders ("the reporter" or "you"), including customers, partners, and security researchers, to identify and responsibly disclose potential security vulnerabilities.

This policy explains how to report potential security vulnerabilities affecting Bruker products and systems and services and describes Bruker's coordinated vulnerability disclosure process.

This policy forms part of Bruker's product security framework and supports compliance with applicable legal and regulatory requirements, including the Cyber Resilience Act, EU-Regulation 2024/2847 (CRA).

Bruker does not operate a bug bounty program. Submission of a report does not give rise to any entitlement to compensation, reward, reimbursement, or other benefit, whether monetary or non-monetary.

By taking part in this vulnerability disclosure program, you agree to follow the terms and conditions described in this policy and confirm that you have read and understood them.

Products and services in scope

This policy applies to all products, systems and services and corresponding websites provided or maintained by Bruker that are within the scope of Bruker's Product Security Incident

Response Team (PSIRT) processes and applicable cybersecurity and product security requirements, including products with digital elements subject to the Cyber Resilience Act.

Certain Bruker affiliates, subsidiaries, acquired businesses, or websites may be subject to separate vulnerability disclosure processes. If you are unsure whether a product, service, or website is covered by this policy, please contact us through the reporting channel identified below.

Scope of vulnerability disclosure

We welcome reports of potential security vulnerabilities affecting the confidentiality, integrity, availability, authenticity, or safety of Bruker products, system or services. This includes, but is not limited to, vulnerabilities related to authentication, authorization, data exposure, and injection attacks. If there is a vulnerability not in scope that you would like to report, please contact us to discuss it first.

Exclusions from the scope

The following reports are not within the scope of this policy and are not eligible for submitting:

- Products or versions that are out of support
- Social-Engineering Attacks
- Denial-of-Service-Tests
- Software version disclosure
- Clickjacking on non-sensitive pages

• Reporting

Please report vulnerabilities by either sending an email to psirt@bruker.com or via the vulnerability reporting form at https://www.bruker.com/en/legal/cyber-resilience.html

Reports can also be sent anonymously. However, anonymous reporting may limit Bruker's ability to investigate, validate, respond to, or provide updates regarding the reported issue.

Please do not include sensitive information, including personal data, confidential information, customer data, credentials, trade secrets, or other proprietary information, in your report unless strictly necessary to demonstrate the reported vulnerability. Where possible, such information should be removed, anonymized, or redacted prior to submission.

When submitting a product vulnerability report, contact us in English or German and include the following information:

- Name and version of the affected product
- Nature of vulnerability and its impact on the product
- Detailed description of the steps required to reproduce the vulnerability (proof-of-concept scripts or screenshots are helpful)
- Date and time of discovery
- Name of the reporter and contact information (email address, phone number) - unless you wish to remain anonymous

Important notice

Submission of a report does not create any contractual relationship, contractual obligation, service commitment, or expectation of a specific response, remediation, or disclosure outcome.

Reports are reviewed and prioritised based on their nature, severity, completeness, and potential impact and may be closed where they are determined to be out of scope, unsupported, non-reproducible, duplicate, or otherwise not actionable.

What we expect from you

- You shall comply with this policy and any applicable laws and regulations.
- Your primary goal during security research shall be good faith testing, investigation or identification of security vulnerabilities.
- You are encouraged to refrain from public disclosure until Bruker has had a reasonable opportunity to analyze and, where appropriate, remediate the reported vulnerability.
- You shall use testing methods and proof-of-concept techniques only to the extent reasonably necessary to prove the existence of a vulnerability.
- You shall not submit large volumes of low-quality, automated, duplicate, or intentionally misleading reports.
- This policy is intended for external reporters. Bruker employees should report potential security vulnerabilities through the applicable internal reporting channels.
- You shall not conduct denial-of-service testing, social-engineering activities, spam or phishing campaigns, or physical security testing of Bruker facilities.

Safe harbor

Bruker considers security research conducted in accordance with this policy to be authorized. Bruker will not take legal action against individuals who:

- act in good faith;
- comply with applicable laws and this policy;
- avoid causing harm, disruption, privacy violations, or unauthorized access to data beyond what is reasonably necessary to demonstrate the existence of a vulnerability; and
- promptly report identified vulnerabilities through Bruker's designated reporting channels.

This safe harbor does not apply to activities involving malicious intent, criminal conduct, extortion, threats, data exfiltration, service disruption, or other unlawful activity.

Limitation of liability

Any information, updates, or fixes provided through this CVD process are offered on an "as-is" basis without warranties of any kind. We assume no liability for indirect, incidental, or consequential damages, or lost profits resulting from the exploitation of a reported vulnerability or the use of this CVD policy. This limitation does not apply to damages caused by willful misconduct, gross negligence, or injury to life, body, or health.

What you can expect from us

- Bruker will handle submitted information in accordance with applicable legal requirements and internal confidentiality and information protection practices.

-Bruker Confidential-

- Personal data will be processed in accordance with applicable data protection laws and may be disclosed where required for vulnerability assessment, remediation, legal compliance, or regulatory reporting purposes.
- Where contact information is provided, Bruker aims to acknowledge receipt of valid vulnerability reports within five (5) business days.
- Bruker will review reported vulnerabilities and may communicate status updates where appropriate and practicable.
- Bruker may publish a security advisory or other disclosure regarding a reported vulnerability where appropriate and in accordance with applicable legal, regulatory, and operational considerations.

Formal case closure

A vulnerability case is formally closed only when the following criteria are met:

- Remediation: Appropriate remediation measures, mitigation guidance, or other risk-treatment actions have been determined and implemented where warranted.
- CRA Notification: Mandatory reports to CSIRTs/ENISA under Art. 14 CRA are fully submitted.
- Disclosure: Any security advisory, notification, or disclosure activity has been completed, where applicable.
- Documentation: The entire case lifecycle is archived for regulatory compliance and audit readiness.

Note: We close a report at once, without a patch, if it turns out to be a false positive or out of scope.

Disclaimer

This policy is provided for informational purposes only and may be updated or modified by Bruker at any time.

Nothing in this policy creates contractual rights or obligations between Bruker and any reporter.

Bruker reserves the right to determine, in its sole discretion and in accordance with applicable legal requirements, how reported vulnerabilities are assessed, prioritised, remediated, disclosed, and closed.

-Bruker Confidential-