Coordinated Vulnerability Disclosure Policy

Product Security Incident Response Team (PSIRT)

Version: 1.02, *Effective date: 14.Sept 2026*

1. Purpose

E+H Metrology is committed to the security of our products and the protection of our customers. This Coordinated Vulnerability Disclosure (CVD) Policy describes how security researchers, customers, and other members of the public can report suspected security vulnerabilities in our products to us, and what they can expect from us in return.

This policy supports our obligations under Regulation (EU) 2024/2847 (the Cyber Resilience Act), Annex I, Part II, which requires manufacturers of products with digital elements to establish and enforce a coordinated vulnerability disclosure policy.

2. Scope

This policy applies to all E+H Metrology products, including:

- The MX product family (handheld measurement devices and automated sorting systems)
- The AZ product family (analog measurement systems)
- E+H Metrology operating software and visualization software

This policy does not cover vulnerabilities in third-party products, corporate IT infrastructure not directly related to a shipped product, or our public website, unless such a vulnerability directly affects the security of an E+H Metrology product. If you discover an issue outside this scope, please still contact us – we will route it appropriately.

3. How to Report a Vulnerability

If you believe you have found a security vulnerability in an E+H Metrology product, please report it to our Product Security Incident Response Team (PSIRT) using one of the following channels:

- Email: cra-reporting@eh-metrology.com (PGP encryption available, see Section 10)
- Phone: +49 (0)721 83118-900

Please do not disclose the vulnerability publicly or to any third party until we have had the opportunity to investigate and address it, in line with the coordinated disclosure timeline described in Section 6.

Version	1-02	Class:	Public	Date Creation:	2026-09-02
Changed by:		Annot:		Created by:	KDR
Checked by:		Annot:		Released by:	KDR

4. What to Include in Your Report

To help us investigate efficiently, please include as much of the following information as possible:

- The affected product(s) and, if known, the firmware/software version
- A description of the vulnerability and its potential impact
- Step-by-step instructions to reproduce the issue
- Any proof-of-concept code, screenshots, or logs (kept to the minimum necessary to demonstrate the issue)
- Your preferred contact details and, if applicable, your PGP public key

5. Our Commitment to You

When you report a vulnerability to us in good faith and in accordance with this policy, we commit to:

- Acknowledge receipt of your report within 3 business days
- Provide an initial assessment (validity, severity) within 10 business days
- Keep you informed of our progress at reasonable intervals
- Work with you toward a coordinated public disclosure timeline, generally targeting remediation within 90 days of confirmation, depending on complexity and severity
- Credit you for your discovery, if you wish (see Section 8)

These timeframes are targets and may vary depending on the complexity of the vulnerability, the need to coordinate with third-party component suppliers, and the number of affected products.

6. Coordinated Disclosure & Safe Harbor

We ask that you:

- Give us a reasonable opportunity to investigate and remediate an issue before disclosing it publicly (generally 90 days from your initial report, unless we agree on a different timeline together)
- Avoid privacy violations, destruction of data, or interruption or degradation of our services during your research
- Only interact with test accounts, test environments, or your own equipment – never with production systems belonging to other customers
- Not exploit a vulnerability beyond what is necessary to demonstrate it (no further access, exfiltration, or modification of data than strictly required for proof of concept)

If you make a good-faith effort to comply with this policy during your security research, we will not pursue legal action against you for that research, and we will consider your actions to be authorized. If legal action is initiated by a third party against you for activities conducted in accordance with this policy, we will make this authorization known.

7. Rules of Engagement

The following activities are out of scope and not authorized under this policy:

- Denial-of-service testing
- Physical attacks against E+H Metrology facilities, employees, or customer installations
- Social engineering of E+H Metrology staff, contractors, or customers
- Testing against production systems or installations belonging to E+H Metrology customers without their explicit permission

8. Recognition

With your permission, we are happy to publicly acknowledge your contribution once a fix has been released. We do not currently operate a paid bug bounty program.

9. Legal

This policy does not grant you permission to act in any manner that is inconsistent with applicable law, or which we have not expressly authorized in this document. Nothing in this policy shall be construed as a waiver of any right E+H Metrology may otherwise have.

10. Encryption

Team: Product Security Incident Response Team (PSIRT)

Once contacted through our web form, we will contact you by mail.

For sensitive reports, we encourage the use of PGP encryption:

PGP Fingerprint: 1D5F 742D 861D 1F0F E092 3A7D 6FFC 84D1 027E E0FF

Key valid until: 02 September 2029