RENA Technologies GmbH

Coordinated Vulnerability Disclosure (CVD) Policy

in accordance with Art. 13(8) of the EU Cyber Resilience Act (CRA), Regulation (EU) 2024/2847

Document type	Policy – publicly accessible (in accordance with Art. 13(8) CRA)
Version	1.0 (draft)
Status	In progress
Created by	Andreas Heeren, VP Engineering
Responsible	Andreas Heeren
Created on	September 7, 2026
Last revised	September 7, 2026
Contact address	https://www.rena.com/en/contact/vulnerability-reporting-form
Classification	Public
Applicable standards	EU CRA (EU) 2024/2847 / BSI TR-03183-3 / ISO/IEC 29147

1. Purpose and scope

RENA Technologies GmbH (hereinafter referred to as "RENA") takes the security of its products and digital services seriously. This Policy sets out how security researchers, customers, and other third parties can responsibly report vulnerabilities in RENA products and how RENA handles reports received.

The Policy applies to the following products and systems:

- Network-connected wet process systems (network-connected machine control systems, remote-access interfaces, industrial IoT components, network-connected PLC/HMI systems)
- Software components and firmware used in the aforementioned products

Expressly out of scope:

- Purely mechanical components without digital connectivity
- RENA's general IT infrastructure (ERP, office IT systems, internal network infrastructure)
- Products operated entirely outside the EU market

2. Contact address for reporting vulnerabilities

Vulnerabilities can be reported through the following channel:

Contact form	https://www.rena.com/en/contact/vulnerability-reporting-form
Languages	German, English
Availability	24/7; processing on working days within two business days

3. Reporting process and timeframes

For all vulnerability reports received, RENA undertakes to:

Step	Action	Timeframe
1	Acknowledge receipt to the reporter	**≤ 5 working days**
2	Conduct an initial plausibility check; severity assessment (CVSS v3.1)	**≤ 15 days**
3	Inform the reporter of the outcome of the initial assessment	**≤ 20 days**
4	Develop and test a fix (prioritized by severity: critical < 30 days, high < 60 days)	**According to severity**
5	Provide a security update to affected users – before public disclosure	**Before disclosure**

6	Coordinate public disclosure in consultation with the reporter and, if relevant, BSI/CSIRT. Standard deadline: 90 days from receipt of the report. ⚠ Internal review recommendation: Consider agreeing a flexible timeline with BSI/CSIRT (rather than a fixed deadline).	**90 days (standard)** **⚠ Alternative: agree a flexible review timeline with BSI/CSIRT**

4. Reporting requirements

A complete report should include the following information (if available and known):

- Affected product/system and version
- Description of the vulnerability and possible impact
- Steps to reproduce (proof of concept, if available)
- Testing or analysis methodology used
- Contact details for queries (optional – anonymous reports are expressly permitted)

RENA also accepts incomplete reports. It is not the reporter's responsibility to identify the cause in a specific internal component or to forward the report to suppliers – that is solely RENA's responsibility.

5. Safe harbor – protection for security researchers

RENA undertakes that persons reporting vulnerabilities in accordance with this Policy will not be subject to criminal or civil proceedings by RENA, provided that they do not (a) process third-party personal data without authorization, (b) affect system operation, (c) cause damage beyond what is strictly necessary to demonstrate the vulnerability, or (d) disclose the vulnerability to third parties before RENA has produced a fix or the disclosure deadline has expired.

6. Anonymity and recognition

Anonymous reports are expressly permitted and given equal consideration. Reporters who wish to be named are – at their express request – mentioned by RENA in the security advisory after the vulnerability has been successfully validated and remedied.

7. Third-party and open-source components

If a reported vulnerability affects a third-party or open-source component, RENA coordinates the communication with the respective manufacturer or project community. The reporter is kept informed of the progress of the coordination. RENA is the single point of contact for the reporter – regardless of the cause of the vulnerability.

8. National CSIRT coordination (BSI)

RENA designates the Federal Office for Information Security (BSI) as the competent national CSIRT pursuant to Art. 13(6) CRA and Art. 12 of the NIS2 Directive. In the case of actively exploited vulnerabilities, RENA coordinates the disclosure with BSI. If necessary, reporters may, alternatively or additionally, report vulnerabilities directly to BSI (https://www.bsi.bund.de).

9. Effective date, review, and versioning

This Policy takes effect on the date of its initial publication. It shall be reviewed at least yearly and modified as necessary (Section 4.4.1 a/c of BSI TR-03183-3). The last modification date is shown in the document header at the top.

Version	Date	Author	Revision
1.0	September 10, 2026	Andreas Heeren	**Initial publication**