RENA Technologies GmbH

Coordinated Vulnerability Disclosure (CVD) Policy

gemäß EU Cyber Resilience Act (CRA), Verordnung (EU) 2024/2847, Art. 13 Abs. 8

Dokumenttyp	Policy – öffentlich zugänglich (gemäß CRA Art. 13 Abs. 8)
Version	1.0
Status	In Bearbeitung
Erstellt von	Andreas Heeren, VP Engineering
Verantwortlich	Andreas Heeren
Erstellt am	07.09.2026
Letzte Überarbeitung	07.09.2026
Kontaktadresse	https://www.rena.com/en/contact/vulnerability-reporting-form
Klassifizierung	Öffentlich
Normgrundlage	EU CRA (EU) 2024/2847 / BSI TR-03183-3 / ISO/IEC 29147

1. Zweck und Geltungsbereich

RENA Technologies GmbH (nachfolgend "RENA") nimmt die Sicherheit ihrer Produkte und digitalen Dienste ernst. Diese Policy legt fest, wie Sicherheitsforscher, Kunden und sonstige Dritte Schwachstellen in RENA-Produkten verantwortungsvoll melden können und wie RENA mit eingegangenen Meldungen umgeht.

Die Policy gilt für folgende Produkte und Systeme:

- Nassprozess-Anlagen mit Netzwerkanbindung (vernetzte Maschinensteuerungen, Remote-Access-Schnittstellen, industrielle IoT-Komponenten, SPS/HMI mit Netzwerkanbindung)
- Software-Komponenten und Firmware, die in den oben genannten Produkten eingesetzt werden

Ausdrücklich nicht im Scope:

- Rein mechanische Komponenten ohne digitale Vernetzung
- Allgemeine IT-Infrastruktur von RENA (ERP, Office-IT, interne Netzwerkinfrastruktur)
- Produkte, die vollständig außerhalb des EU-Markts betrieben werden

2. Kontaktadresse für Schwachstellenmeldungen

Schwachstellen können über folgenden Kanal gemeldet werden:

Kontaktformular	https://www.rena.com/en/contact/vulnerability-reporting-form
Sprachen	Deutsch, Englisch
Verfügbarkeit	24/7; Bearbeitung an Werktagen innerhalb von 2 Geschäftstagen

3. Meldeprozess und Fristen

RENA verpflichtet sich zur Bearbeitung aller eingehenden Schwachstellenmeldungen nach folgendem Prozess:

Schritt	Maßnahme / Aktivität	Frist
1	Eingangsbestätigung an die meldende Person	**≤ 5 Werktage**
2	Initiale Plausibilitätsprüfung; Schweregradbewertung (CVSS v3.1)	**≤ 15 Tage**
3	Rückmeldung an die meldende Person über Ergebnis der Erstbewertung	**≤ 20 Tage**
4	Entwicklung und Test eines Fixes (priorisiert nach Schweregrad: Kritisch < 30 Tage, Hoch < 60 Tage)	**Nach Schweregrad**

5	Bereitstellung des Sicherheitsupdates an betroffene Nutzer – vor öffentlicher Offenlegung	**Vor Offenlegung**
6	Koordinierte öffentliche Offenlegung in Abstimmung mit meldender Person und ggf. BSI/CSIRT. Standard-Deadline: 90 Tage ab Eingang der Meldung. ⚠ Interne Prüfempfehlung: Erwägen Sie eine flexible Abstimmung mit dem BSI/CSIRT (statt fester Deadline).	**90 Tage (Standard)** **⚠ Alternativ: flexibel in Abstimmung mit BSI/CSIRT prüfen**

4. Anforderungen an die Meldung

Eine vollständige Meldung sollte folgende Informationen enthalten (soweit verfügbar und bekannt):

- Betroffenes Produkt / System und Versionsstand
- Beschreibung der Schwachstelle und möglicher Auswirkungen
- Schritte zur Reproduktion (Proof of Concept, soweit vorhanden)
- Eingesetzte Test- oder Analysemethodik
- Kontaktdaten für Rückfragen (optional – anonyme Meldung ist ausdrücklich möglich)

RENA nimmt auch unvollständige Meldungen entgegen. Es ist nicht Aufgabe der meldenden Person, die Ursache in einer spezifischen internen Komponente zu identifizieren oder die Meldung an Zulieferer weiterzuleiten – dies liegt ausschließlich in der Verantwortung von RENA.

5. Safe Harbor – Schutz für Sicherheitsforscher

RENA verpflichtet sich: Personen, die Schwachstellen im Einklang mit dieser Policy melden, werden von RENA weder strafrechtlich noch zivilrechtlich verfolgt, sofern sie (a) keine personenbezogenen Daten Dritter unbefugt verarbeiten, (b) den Betrieb von Systemen nicht beeinträchtigen, (c) keinen Schaden über das zur Demonstration erforderliche Minimum verursachen und (d) die Schwachstelle nicht an Dritte weitergeben, bevor RENA eine Lösung bereitgestellt oder die Offenlegungsfrist verstrichen ist.

6. Anonymität und Anerkennung

Anonyme Meldungen sind ausdrücklich möglich und werden gleichwertig bearbeitet. Meldende Personen, die namentlich genannt werden möchten, werden nach erfolgreicher Validierung und Behebung der Schwachstelle – auf ausdrücklicher Wunsch – in der Sicherheitsmitteilung von RENA erwähnt.

7. Drittanbieter- und Open-Source-Komponenten

Betrifft eine gemeldete Schwachstelle eine Drittanbieter- oder Open-Source-Komponente, koordiniert RENA die Kommunikation mit dem jeweiligen Hersteller bzw. der Projekt-Community. Die meldende Person wird über den Stand der Koordination informiert. RENA ist gegenüber der meldenden Person der alleinige Ansprechpartner – unabhängig davon, wo die Ursache der Schwachstelle liegt.

8. Nationale CSIRT-Koordination (BSI)

RENA benennt das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zuständiges nationales CSIRT gemäß CRA Art. 13 Abs. 6 und NIS-2-Richtlinie Art. 12. Bei aktiv ausgenutzten Schwachstellen koordiniert RENA die Offenlegung in Abstimmung mit dem BSI. Meldende Personen können Schwachstellen bei Bedarf alternativ oder zusätzlich direkt an das BSI melden (https://www.bsi.bund.de).

9. Geltung, Überprüfung und Versionierung

Diese Policy tritt mit Datum der Erstveröffentlichung in Kraft. Sie wird mindestens jährlich überprüft und bei Bedarf aktualisiert (BSI TR-03183-3, Abschnitt 4.4.1 a/c). Das Datum der letzten Änderung ist oben im Dokumentkopf ausgewiesen.

Version	Datum	Autor	Änderung

1.0	10.09.2026	Andreas Heeren	**Erstveröffentlichung**