CVD Policy

(Coordinated Vulnerability Disclosure Policy)

KROHNE Group · Integrated Management System



DOCUMENT IDENTIFICATION	
Document ID / Status	QSCH-6.3-000468
Document Title	CVD Policy
Document Type	Policy
Version	1
Scope	KROHNE Group
STATUS & CLASSIFICATION	
Confidentiality	Public
Last Review Date	2026-10-05
Next Review Due Date	2027-10-05
OWNERSHIP & APPROVAL	
Document Owner	Mamberger, Sergej (Cyber Security Engineer)
Process Owner	Hottgenroth, Wolfgang (Corporate Security Expert)
Reviewers	Niermann, Benedikt (VP QHSE & Business Process Management)
Approver	Bilgic, Attila (CEO)

This is a controlled document. Printed or downloaded copies are considered uncontrolled. The metadata for this document is maintained and controlled in the document management system.
This document is based on a template provided by CERT@VDE.

Content

1. Introduction and Scope 4
2. Contact channels for reporting 4
3. Content of a vulnerability report 4
4. Process and ongoing communication 4
5. Secure and anonymous communication 4
6. Disclosure strategy and embargo 5
7. Publication and recognition 5
8. Legal framework 5

1. Introduction and Scope

At KROHNE Group, the security of our products with digital elements is a high priority. This policy describes how you can report a potential vulnerability in our products to us and how we handle your report. We welcome reports from security researchers, customers, partners and the public.

Scope: This policy applies to all KROHNE products with digital elements currently in the EU market.

2. Contact channels for reporting

You can reach our security team through the following channels:

- Email: psirt@krohne.com (role-based, not tied to an individual)
- Web form: https://www.krohne.com/en-de/company/cybersecurity/report-vulnerabilities-or-incidents

Our security.txt according to RFC 9116: https://www.krohne.com/.well-known/security.txt.

3. Content of a vulnerability report

So that we can process your report quickly, please provide – where possible:

- Affected product, version or build, and environment
- Description of the vulnerability and its potential impact
- Steps to reproduce (proof of concept), if available
- Your contact details for follow-up (optional – anonymous reporting is possible, see section 5)

4. Process and ongoing communication

After receiving your report, we proceed as follows:

1. Acknowledgement of receipt within 3 business days, assigning a unique tracking number.
2. Assessment and verification of the reported vulnerability.
3. Status updates
    1. Updates every two weeks
    2. Final Report once the incident is closed
4. Mitigation, Remediation and publication in accordance with sections 6–7.

5. Secure and anonymous communication

Vulnerability information is sensitive. For confidential transmission we offer:

- PGP/GPG: Public key with Key-ID: 40A4B5949CA862DC and Fingerprint: 298B 229F 6DBE F3C0 B064 985A 40A4 B594 9CA8 62DC, available at https://dam.krohne.com/raw/upload/do-other/krohne-psirt-public.asc
- HTTPS web form (TLS-encrypted)

Anonymous reporting: You can also report anonymously. We accept reports even when no secure channel can be used.

6. Disclosure strategy and embargo

We follow the principle of coordinated disclosure and disclose vulnerability details after remediation, mitigation or other appropriate risk-reduction measures are available.

We agree on an appropriate embargo period of 90 days, which can be adjusted case by case depending on complexity and criticality.

7. Publication and recognition

After remediation or mitigation we publish a security advisory. You can find our published advisories at https://www.krohne.com/en/company/cybersecurity/overview-advisories; they are additionally provided or linked via the CERT@VDE advisory portal (https://certvde.com/en/advisories/). Recognition is optional and the reporter will be credited upon request and reporter's consent.

Hint: We run no bug bounty program.

8. Legal framework

KROHNE acknowledges that vulnerabilities may be discovered in certain legitimate contexts, such as academic research, coordinated audits conducted by customers and partners, or incidental discovery in the normal use of our products. This policy is not an invitation to conduct unsolicited security testing on our systems or products and does not establish a bug bounty program.

We will not initiate legal action against individuals who discover vulnerabilities within one of the contexts described above and report them in good faith and in accordance with the principles of this policy, without violating privacy, destroying data, interrupting services, or causing harm to users.

If you inadvertently gain access to sensitive information during such research, we ask that you stop testing immediately, refrain from further access, and report the incident to us without delay. Information about reported vulnerabilities must be kept confidential until remediation or the publication of mitigations, as well as disclosure, have taken place.

Nothing in this policy authorizes activities that violate applicable law or intentionally cause harm to KROHNE, its customers, or third parties.