Coordinated Vulnerability Disclosure Policy

Hch. Kündig & Cie. AG — Kündig Control Systems (KCS)

Scope: All KCS products with digital elements

Legal basis: Regulation (EU) 2024/2847 (Cyber Resilience Act), Art. 13 Para. 6

Version: 1.1 | **Date:** 2026-05-07

1. Introduction

Hch. Kündig & Cie. AG takes the security of its products seriously. Its Kündig Control Systems (KCS) division welcomes reports from security researchers, customers and the public regarding potential vulnerabilities in KCS products.

This CVD Policy describes how vulnerabilities can be reported to KCS, how KCS handles them, and what reporters can expect from the process.

2. Contact

Channel	Address
E-mail (preferred)	security@gauge.ch
Subject line	[SECURITY] <Product name> <Short description>

All reports are treated confidentially.

Response time: KCS will acknowledge receipt within **5 business days**.

3. Scope

This policy applies to vulnerabilities in products distributed by KCS.

Out of scope:

- Physical security of KCS office premises
- Vulnerabilities in third-party products that are not part of a KCS product
- Social engineering against KCS employees

4. Our Expectations of Reporters (Safe Harbour)

Hch. Kündig & Cie. AG / KCS commits to **not pursuing legal action** against individuals who act in good faith and in accordance with this policy, provided the following rules are observed:

Permitted:

- ✓ Testing vulnerabilities on your own systems or with explicit written permission
- ✓ Reporting found vulnerabilities to security@gauge.ch
- ✓ Coordinated disclosure in agreement with KCS

Not permitted:

- ✗ Accessing customer data or third-party production systems

✗ Destructive testing (DoS, data destruction)

✗ Public disclosure before the coordination period has elapsed

✗ Exploiting the vulnerability for personal gain

5. Process Upon Receipt of a Report

Step	Deadline	Description
Acknowledgement	5 business days	KCS confirms receipt and provides a tracking ID
Initial assessment	10 business days	KCS evaluates severity and reproducibility
Status update	30 days	KCS informs the reporter of progress
Remediation	By severity	Critical 7d, High 30d, Medium 90d, Low 180d
Coordinated disclosure	After patch release	KCS notifies reporter; joint disclosure possible

6. What KCS Expects from Reporters

- **Coordination:** No public disclosure before the coordination period ends (max. 90 days)
- **Minimally invasive:** No access beyond what is necessary to verify the vulnerability
- **Documentation:** Sufficient information to reproduce the vulnerability
- **Availability:** Reachable for follow-up questions during the coordination period

7. What Reporters Can Expect from KCS

- Prompt acknowledgement of receipt
- Transparent communication on the status of the report
- Credit in the security advisory (optional, with the reporter's consent)
- No legal action for good-faith compliance with this policy

8. Changelog

Version	Date	Change
1.0	2026-04-13	Initial version
1.1	2026-05-07	Separate DE/EN documents

Responsible: Roger Fässler, PSIRT Lead — Hch. Kündig & Cie. AG / Kündig Control Systems (KCS), security@gauge.ch